

Sécurité mobile

La section sur la sécurité mobile comprend des guides pratiques sur un certain nombre d'applications Freeware ou Open Source pour smartphone dont la fonction est d'assurer un usage sécurisé de votre smartphone. De la même manière que les guides pratiques sur les applications informatiques, ils vous guideront à travers les différents procédés de téléchargement et de configuration des applications, par le biais d'instructions étape par étape et de captures d'écran pour une compréhension facile.

Les applications peuvent être téléchargées sous forme de fichiers .apk à partir des sites Internet des développeurs. Pour cela, il suffit de cliquer sur le lien fourni dans le guide correspondant. Elles sont également disponibles dans la boutique en ligne Google Play.

Pour des raisons de sécurité, vous devriez toujours utiliser la plus récente version des programmes présentés ici. La version de certains des programmes présentés ici est peut-être plus récente que celle utilisée lors de la rédaction du guide pratique correspondant. Dans ce cas, l'interface de la nouvelle version peut différer légèrement de celle décrite dans ce guide, mais pas substantiellement.

Les guides pratiques fournis dans la section sur la sécurité mobile sont actuellement uniquement disponibles sur appareils Android. Toutefois, leur utilisation sera bientôt élargie aux applications iPhone.

Android Privacy Guard (APG) pour appareils Android

Short Description:

Android Privacy Guard (APG) est une application Android libre et open source, créée par [Thialfiar](#) ^[1], qui permet de chiffrer et déchiffrer des fichiers individuels et des courriels. Il vise à fournir les appareils Android avec un chiffrement au format **OpenPGP**. Toutefois, toutes les fonctions d'OpenPGP ne sont pas encore en état de marche. Son système de clé publique / clé privée vous permet de chiffrer, déchiffrer et signer des fichiers et des messages. Vous pouvez également l'utiliser sans paire de clés publique/privée pour signer des fichiers individuels avec un chiffrement asymétrique, sécurisant les fichiers au moyen d'un mot de passe ou d'une phrase secrète. Pour tout chiffrement de courriel, nous recommandons de l'utiliser avec **K9**, un client de messagerie Android, pour lequel il existe également un [guide pratique](#) ^[2].

Online Installation Instructions:

Télécharger Android Privacy Guard

À partir du site web officiel

- Lisez l'introduction courte [Guides pratiques](#) ^[3]
- Cliquez sur l'icône **APG** ci-dessous pour ouvrir <http://www.thialfiar.org/projects/apg/>
- *Defilez vers le bas jusqu'à download (téléchargement). Vous pouvez alors scanner le code QR de téléchargement et installation.

À partir de F-Droid (Android FOSS repository)

- Vous pouvez également installer **APG** à partir de [F-Droid](#) ^[4] qui est un marché d'applications libres pour Android
- Une fois installée, cliquez sur Open (ouvrir) pour démarrer l'application

APG:



^[5]

Page d'accueil

- [Page d'accueil d'APG](#) ^[5]
- [Site du développeur d'APG](#) ^[6]

Matériel requis

- Android 1.5 ou plus récent

Versión utilisée dans ce guide

- 1.0.8

Licence

- FOSS (Licence Apache 2.0)

Lecture requise

- Livret pratique, chapitre **3. Créer et sauvegarder des mots de passe sûrs** [7]
- Livret pratique, chapitre **7. Préserver la confidentialité de vos communications sur Internet** [8]
- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** [9]
- Livret pratique, chapitre **11. Utiliser votre smartphone en sécurité (autant que possible...)** [10]

Niveau : 1 : Débutant, 2 : **Moyen** (chiffrement de fichiers), 3 : **Intermédiaire** (chiffrement de courriels), 4 : Expérimenté, 5 : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 10 minutes (chiffrement de fichier)

Ce que vous obtenez en retour :

- La faculté de **chiffrer des fichiers individuels et votre messagerie électronique**

1.1 Ce que vous devez savoir avant de commencer à utiliser cet outil

- **APG** s'intègre au client K9 de messagerie pour Android et fait du chiffrement de courrier électronique un jeu d'enfant. Mais dans un premier lieu, il vous faut savoir comment le chiffrement de courrier électronique fonctionne. Ceci est expliqué dans le chapitre **7.4.Principes de sécurité avancée** [11].
- **APG** peut également servir à chiffrer et déchiffrer des fichiers localement sur votre appareil soit avec une phrase secrète, soit avec une paire de clés publique / privée.

2. Comment installer et utiliser APG

Liste des sections:

- **2.0 Comment installer APG**
- **2.1 Comment utiliser APG pour chiffrer et déchiffrer des fichiers**

2.0 Comment installer APG

Étape 1. Téléchargez l'application à partir de [Google Play](#) [12]. Vous pouvez également télécharger l'application à partir de la [page d'accueil du projet](#) [5].

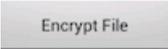
Étape 2. Installez l'application en appuyant sur le bouton **Install** (installer).

Étape 3. Confirmez les autorisations requises par l'application et appuyer sur **Accept and download** (accepter & télécharger).

Étape 4. Appuyez sur *Open* (ouvrir) pour démarrer l'application une première fois.

Ce sont les seules étapes initiales nécessaires au chiffrement d'un fichier avec un mot de passe. Si vous souhaitez utiliser **APG en combinaison avec le client K9 de messagerie**, merci de consulter le [guide pratique K9+APG](#) [2].

2.1 Comment utiliser APG pour chiffrer et déchiffrer des fichiers.

Étape 1. Après avoir ouvert **APG**, appuyez sur .

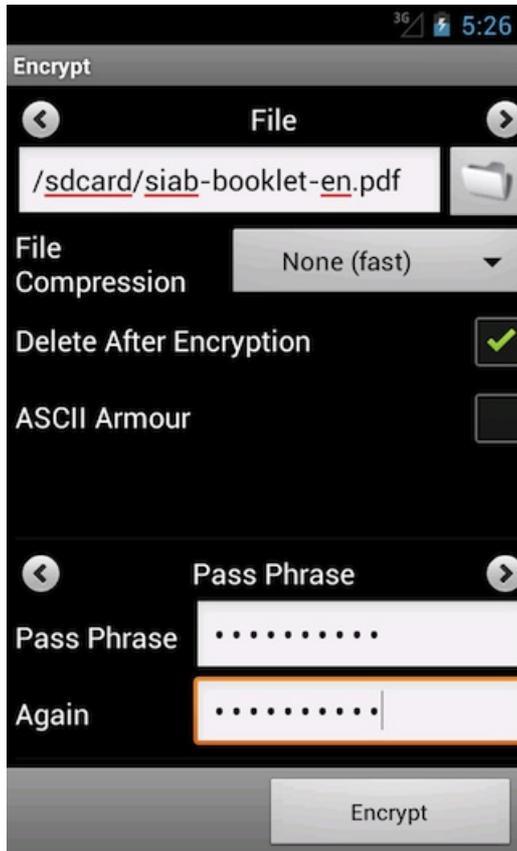
Étape 2. Sélectionnez le fichier à chiffrer en appuyant sur le symbole du dossier, puis sélectionner le fichier dans le gestionnaire de fichiers.

Étape 3. Si vous souhaitez supprimer le fichier original après que celui-ci a été chiffré, **cochez *Delete after encryption*** (supprimer après chiffrement). Ceci est recommandé dans la plupart des cas.

Étape 4. Dans la partie inférieure de la fenêtre, vous avez le choix entre deux méthodes de chiffrement : chiffrement à clé publique (appelé aussi cryptographie asymétrique) ou phrase secrète (que vous sélectionnez en appuyant sur les flèches à gauche ou à droite). Si vous n'avez pas de paire de clés publique / privée et que ce système à clés ne vous est pas familier, sélectionnez *Phrase secrète*.

Étape 5. Entrez une phrase secrète une première, puis une seconde fois. Pour en savoir plus sur les phrases secrètes sûres, consultez le chapitre **3. Créer et sauvegarder des mots de passe sûrs** [7] des guides pratiques.

Étape 6. Appuyez sur *Encrypt* (chiffrer)



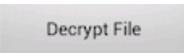
Graphique 1 : Options de chiffrement.

Étape 7. Dans la fenêtre suivante, il vous est demandé de nommer le fichier chiffré. Si vous appuyez sur *OK* sans effectuer aucune modification, alors le dossier chiffré sera sauvegardé dans le dossier **APG** sous son nom original, doté de l'extension ".gpg". **Important** : Si vous modifiez le nom du fichier, assurez-vous qu'il se termine par ".gpg"

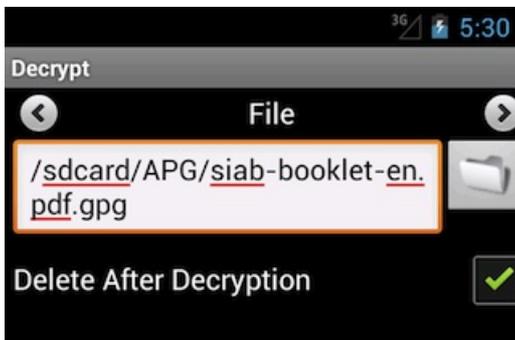


Graphique 2 : Sélectionner le nom du fichier.

Étape 8. L'appareil va commencer à chiffrer le fichier sélectionné. Selon la taille du fichier, cela peut prendre un certain temps.

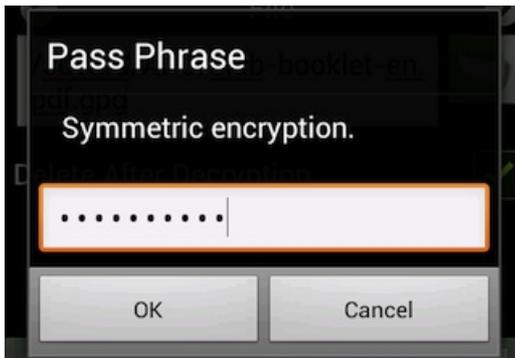
Étape 9. Pour **déchiffrer**, appuyez sur 

Étape 10. **Sélectionnez** le fichier à déchiffrer. Vous pouvez opter pour *delete after decryption* (supprimer après le déchiffrement) si vous souhaitez que le fichier original non chiffré soit supprimé.



Graphique 3 : Sélectionner le fichier à déchiffrer.

Étape 11. Une fenêtre apparaîtra, dans laquelle vous sera demandée votre phrase secrète : **entrez-la** comme demandé.



Graphique 4 : Entrer une phrase secrète.

Étape 12. Une autre fenêtre vous demandera où stocker le fichier déchiffré et sous quel nom. L'emplacement par défaut est à nouveau le dossier **APG**.



Graphique 5 : Sélectionner un nom pour le fichier déchiffré.

Étape 13. L'appareil va commencer à déchiffrer le fichier sélectionné. Selon la taille du fichier, cela peut prendre un certain temps.

Configuration basique des paramètres de sécurité d'un appareil Android

Liste des sections de cette page :

- [1.1 Accès à votre téléphone](#)
- [1.2 Chiffrement de l'appareil](#)
- [1.3 Paramètres du réseau](#)
- [1.4 Paramètres de localisation](#)
- [1.5 Identification de l'appelant](#)

1.1 Accès à votre téléphone

Étape 1. Activez le dispositif *Bloquer la carte SIM* dans *Menu -> Paramètres -> Lieu et sécurité -> Configurer blocage SIM*. Vous devrez alors entrer un code PIN qui bloquera votre carte SIM à chaque nouvel allumage de votre téléphone.

Étape 2. Activez un *verrouillage de l'écran* dans *Paramètres -> Lieu et sécurité -> Verrouillage de l'écran* de sorte qu'un code, un schéma ou un mot de passe soit nécessaire pour déverrouiller l'écran une fois qu'il a été verrouillé. Nous recommandons le verrouillage au moyen d'un code *PIN* ou d'un *mot de passe* dans la mesure où ceux-ci ne sont pas limités dans la longueur. De plus amples informations sur la création de mots de passe sûrs sont disponibles au chapitre

3. Créer et sauvegarder des mots de passe sûrs [7].

Étape 3. Activez la *minuterie de verrouillage de sécurité* qui verrouillera automatiquement votre téléphone au bout d'un certain temps. Vous pouvez spécifier une valeur en fonction de la fréquence selon laquelle vous êtes prêt à avoir à déverrouiller votre téléphone.

1.2 Chiffrement de l'appareil

Étape 4. Si votre appareil utilise la version Android 4.0 ou une version plus récente, vous devriez **activer** le *chiffrement de l'appareil*. Ceci est réalisable en allant à *Paramètres -> Lieu et sécurité -> Chiffrer la tablette*. Cependant, avant de pouvoir utiliser cette fonction, il vous sera demandé de définir un mot de passe de verrouillage de l'écran (comme décrit ci-dessus).

Note : Avant de commencer le processus de chiffrement, assurez-vous que le téléphone est complètement chargé et branché à une source d'alimentation.

1.3 Paramètres de réseau

Étape 5. Désactivez les connexions Wi-Fi et Bluetooth par défaut. Assurez-vous que le *Point d'accès* et le *Modem*, réglables dans le paramètre *Sans fil et réseaux*, sont désactivés lorsque vous ne les utilisez pas.

Étape 6. Si votre appareil est doté de la fonction *Near Field Communication (NFC)*, celle-ci sera activée par défaut, et doit donc être désactivée manuellement.

1.4 Paramètres de localisation

Étape 7. Désactivez la géolocalisation via *satellites GPS et réseaux sans fil* (dans *Services de localisation*) et le transfert de fichiers/données (dans *Gestionnaire de données -> Réception des données*).

Note : Activez les paramètres de localisation dans la mesure de vos besoins. Il est important de veiller à ce que ces services ne fonctionnent pas en arrière-plan par défaut et de réduire ainsi les risques d'être localisé, économiser la batterie et réduire les flux de données indésirables initiés par des applications en arrière-plan ou par votre opérateur de téléphonie mobile à distance .

1.5 Identification de l'appelant

Si vous ne souhaitez pas que l'on voie votre numéro lorsque vous appelez quelqu'un, allez dans *Paramètres -> Paramètres d'appel -> Autres paramètres -> Numéro de l'appelant -> Masquer le numéro*.

Cryptonite pour appareils Android

Short Description:

Cryptonite est une application libre et open source conçue pour les appareils Android par [Christoph Schmidthieber](#) [13]. Elle est basée sur EncFS et TrueCrypt. Vous pouvez parcourir, exporter et ouvrir des répertoires et fichiers chiffrés avec EncFS sur votre téléphone, et ceci vaut pour votre Dropbox également. Sur téléphones rootés, compatibles avec FUSE (p.ex. CyanogenMod), vous pouvez également monter des volumes EncFS et TrueCrypt. Actuellement, TrueCrypt est uniquement disponible en version ligne de commande. Il peut être utilisé pour stocker des fichiers chiffrés.

Online Installation Instructions:

Télécharger Cryptonite

À partir de Google Code

- Lisez l'introduction courte des [guides pratiques](#) [3]
- Cliquez sur l'icône **Cryptonite** ci-dessous pour télécharger le fichier apk de l'application***
- *Cryptonite ne peut toujours pas être téléchargée à partir du marché F-Droid. Nous ajouterons le lien ici dès qu'elle y sera disponible.*

Cryptonite :



[13]

Page d'accueil

- [Page d'accueil de Cryptonite](#) [13]

Matériel requis

- Android 2.2 ou plus récent

Version utilisée dans ce guide

- 0.7.6

Licence

- FOSS (GPLv2)

Lecture requise

- Livret pratique, chapitre [8. Préserver votre anonymat et contourner la censure sur Internet](#) [14]
- Livret pratique, chapitre [9. Utiliser votre téléphone mobile en sécurité \(autant que possible...\)](#) [9]
- Livret pratique, chapitre [11. Utiliser votre smartphone en sécurité \(autant que possible...\)](#) [10]

Niveau 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 10 minutes

Ce que vous obtenez en retour :

- La faculté de **chiffrer** et **déchiffrer** des fichiers localement sur votre appareil ou votre Dropbox ou des services similaires.

1.1 Ce que vous devez savoir sur cet outil avant de commencer

- **Cryptonite** se trouve encore en phase de développement et il se peut que des versions futures aient plus de fonctionnalités.
- Il est déconseillé d'utiliser sa fonction *export* pour Dropbox, étant donné que Dropbox n'est pas un service soucieux de la confidentialité.
- Vous disposerez de toutes les fonctionnalités de TrueCrypt seulement si vous utilisez un firmware de Cyanogenmod. Sans cela, vous ne pourrez ni monter, ni démonter des dossiers chiffrés, mais seulement des fichiers spécifiques.

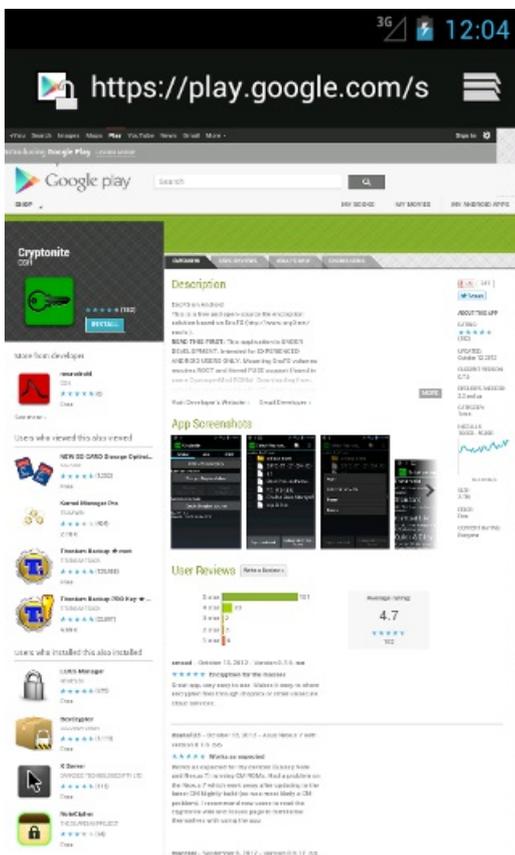
2. Comment installer et utiliser Cryptonite

Liste des sections :

- [2.0 Comment installer Cryptonite](#)
 - [2.1 Comment utiliser Cryptonite pour le chiffrement local de fichiers](#)
 - [2.2 Comment télécharger des fichiers vers le répertoire Cryptonite](#)
-

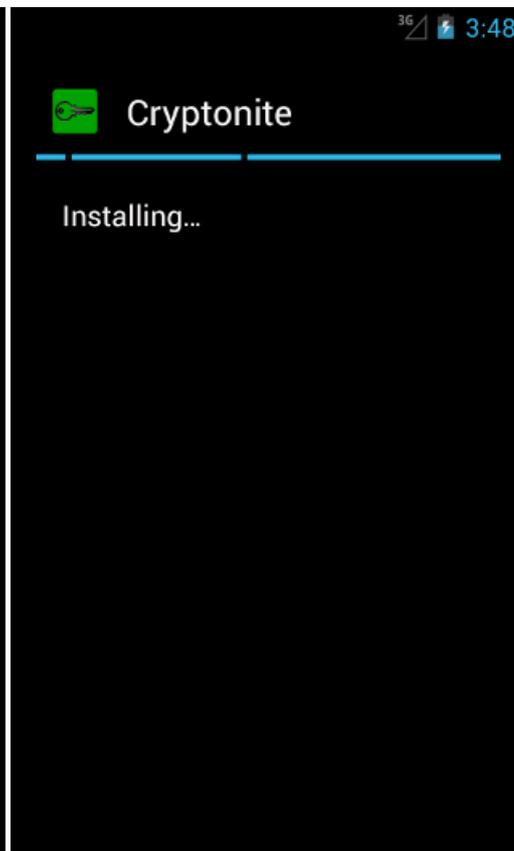
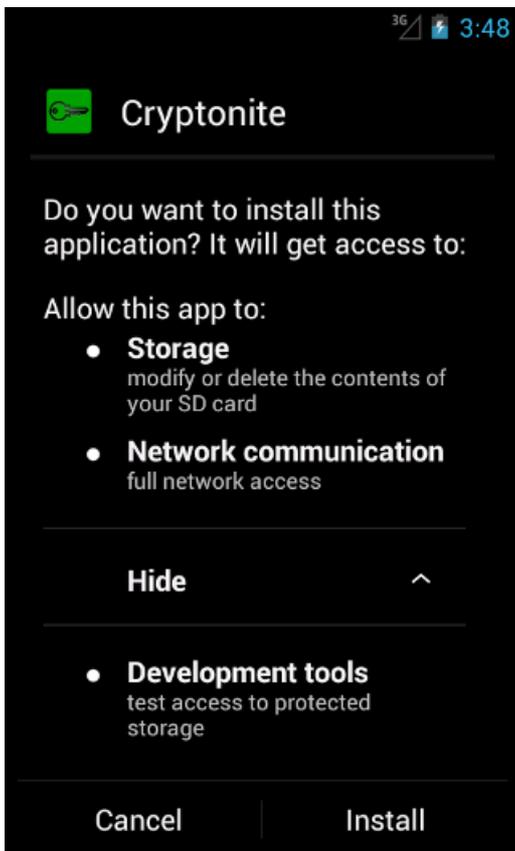
2.0 Comment installer Cryptonite

Étape 1. Téléchargez l'application à partir de la boutique [Google Play](#) [15]



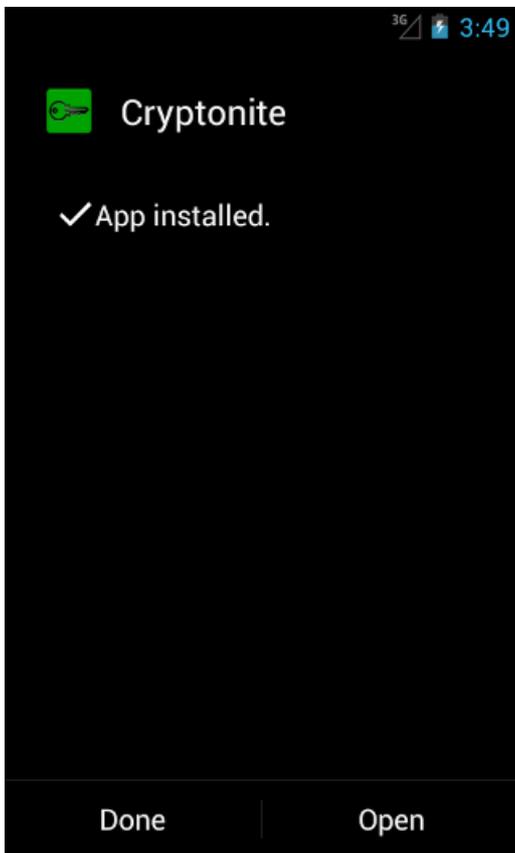
Graphique 1 : Cryptonite dans la boutique Google Play.

Étape 2. Lisez attentivement les autorisations requises par l'application, puis installez-la en appuyant sur le bouton **Install**.



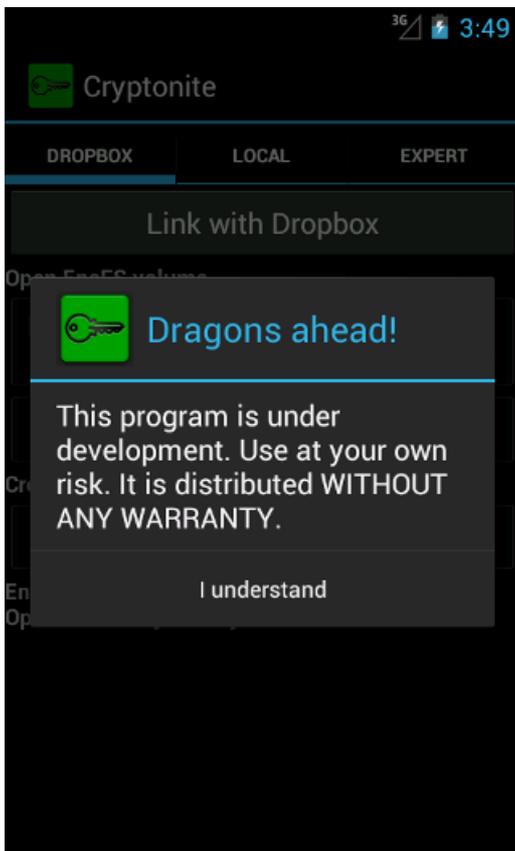
Graphiques 2 et 3 : Autorisations requises et installation.

Étape 3. Appuyez sur *Open* (ouvrir) pour démarrer l'application une première fois.



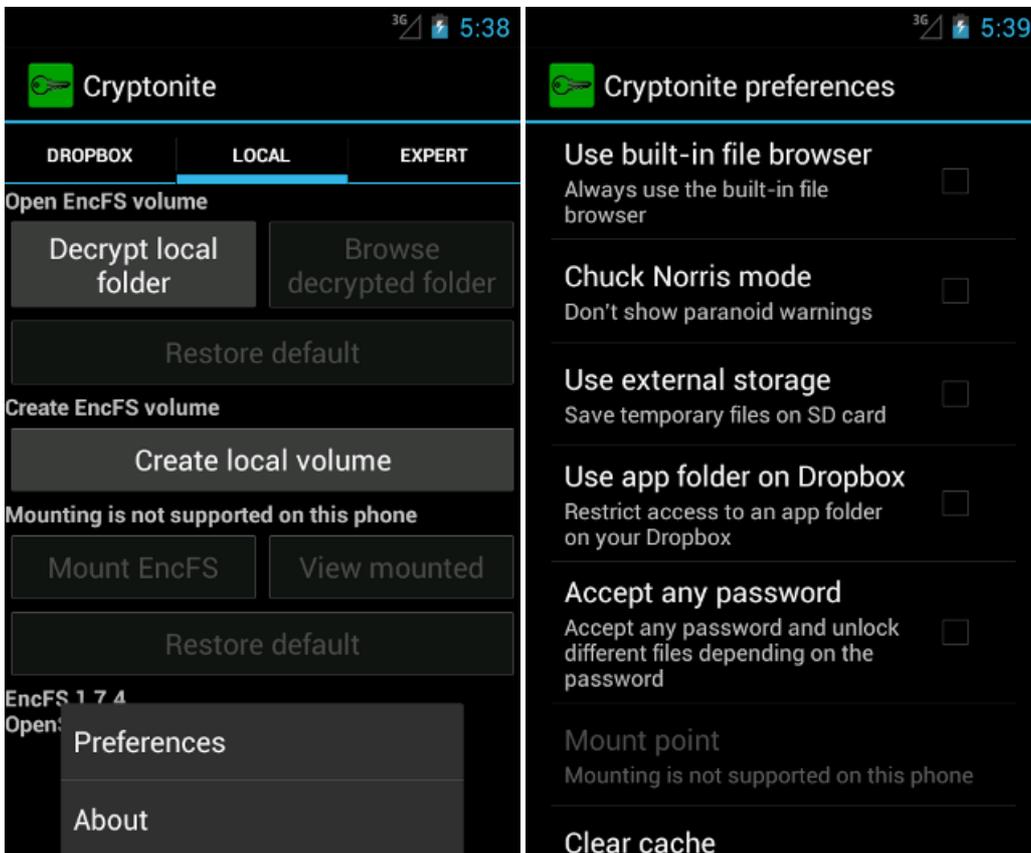
Graphique 4 : Application installée.

Étape 4. Un message apparaîtra comme ci-dessous, **lisez-le** attentivement puis **cliquez** sur *I understand* (je comprends).



Graphique 5 : Avertissement concernant le statut de développement.

Étape 5. Dans l'onglet *Préférences*, assurez-vous que l'option *Use external storage* (utilisation de stockage externe) n'est pas activée.



Graphiques 6 et 7 : Préférences.

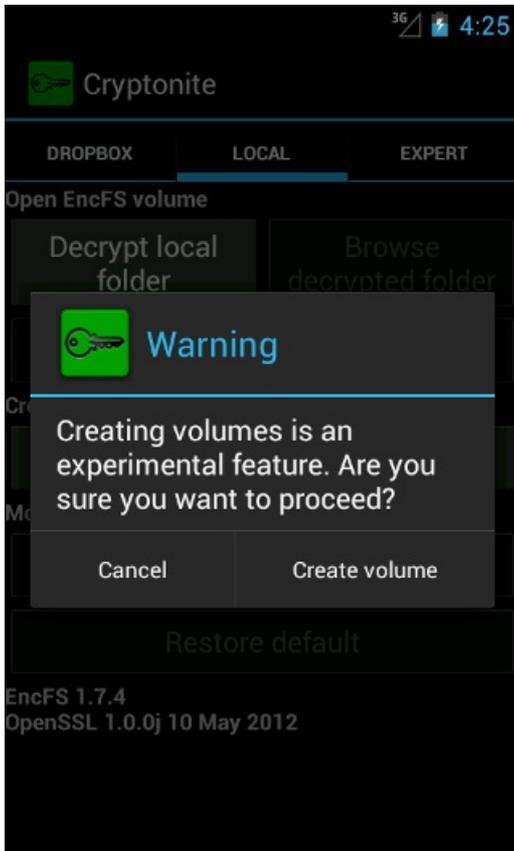
2.1 Comment utiliser Cryptonite pour le chiffrement local de fichiers.

Étape 1. Lors de l'ouverture de **Cryptonite**, un écran présentant trois onglets en haut apparaît : *dropbox*, *local* et *expert*. Nous utilisons ici la première fonctionnalité, c'est à dire *local*. **Appuyez** sur *local*.



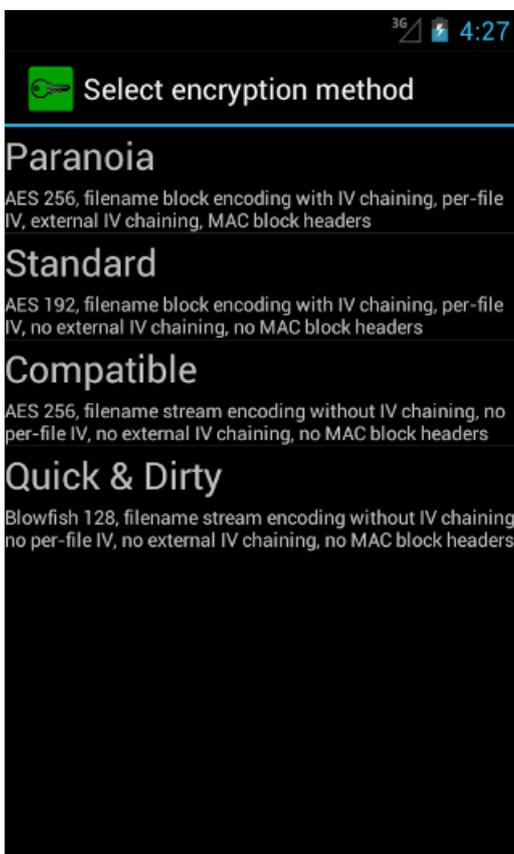
Graphique 8 : Options d'utilisation.

Étape 2. Pour créer un volume chiffré, **appuyez** sur *Create local volume* (créer un volume local). Un message apparaîtra comme ci-dessous, lisez-le attentivement, puis appuyez sur **create a volume** (créer un volume).



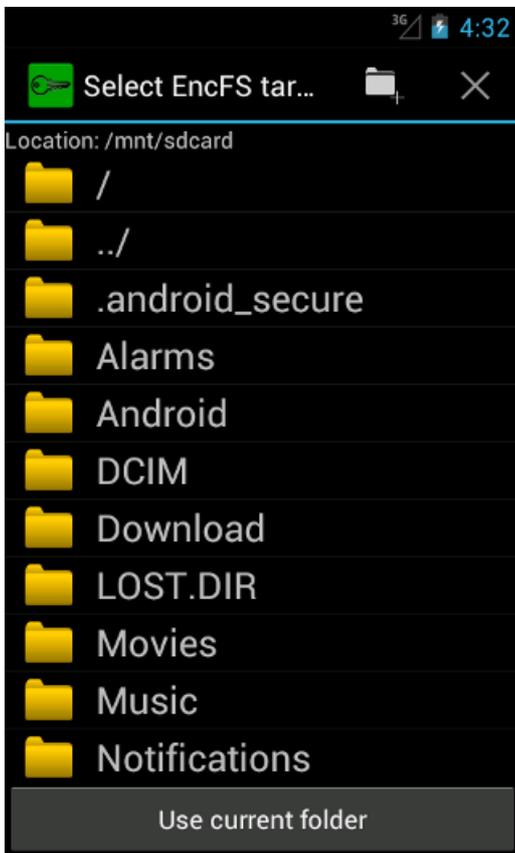
Graphique 9 : Avertissement concernant la création de volumes.

Étape 3. Choisissez parmi les différentes catégories de chiffrement. Nous recommandons *Standard* ou *Paranoïa*.



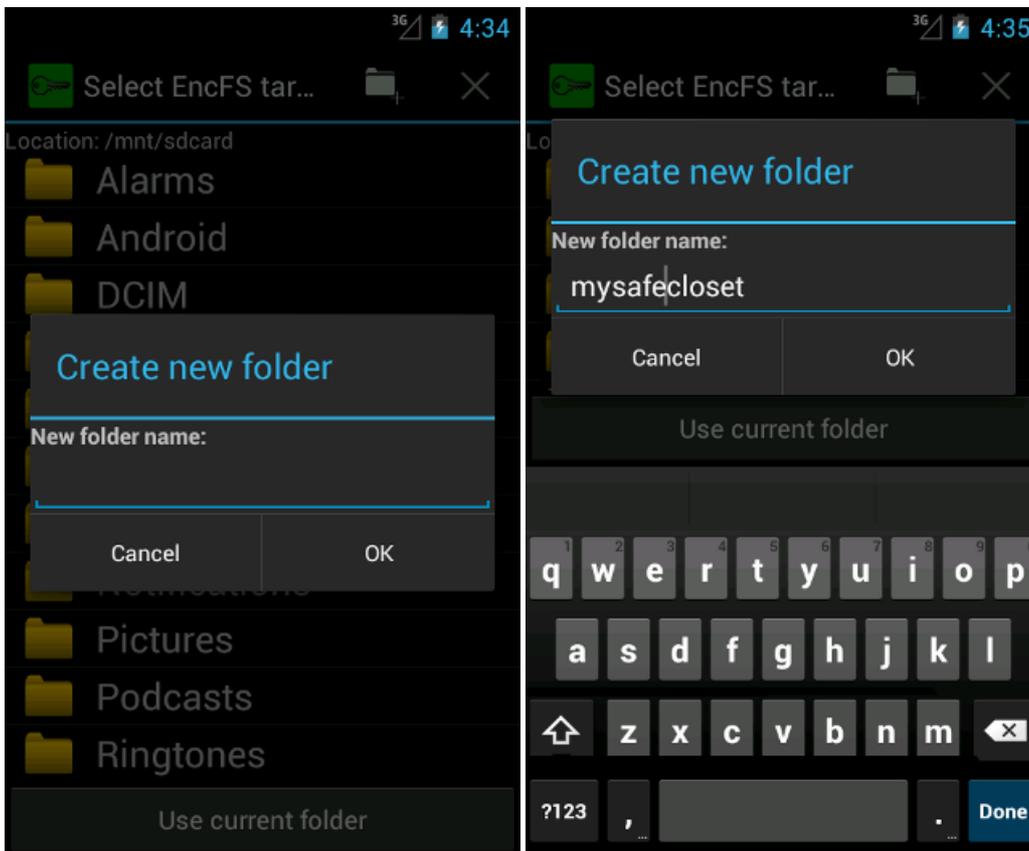
Graphique 10 : Méthodes de chiffrement.

Étape 4. Un explorateur de fichiers s'ouvre. Sélectionnez un dossier qui sert de lieu de chiffrement. Rappelez-vous de quel dossier il s'agit ! Sinon, vous pouvez créer un nouveau dossier en cliquant sur  en haut à droite de l'écran.



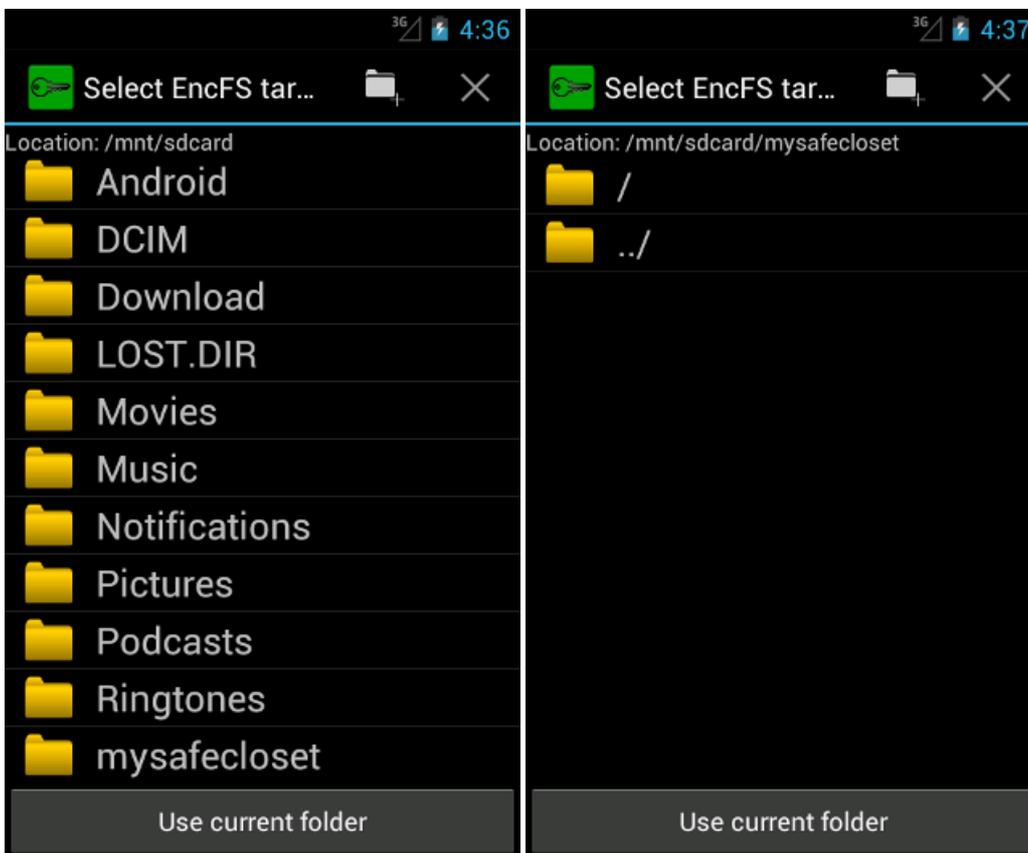
Graphique 11 : Sélectionner un dossier.

Étape 5. Si vous créez un nouveau dossier, **entrez** son nom comme montré ci-dessous.



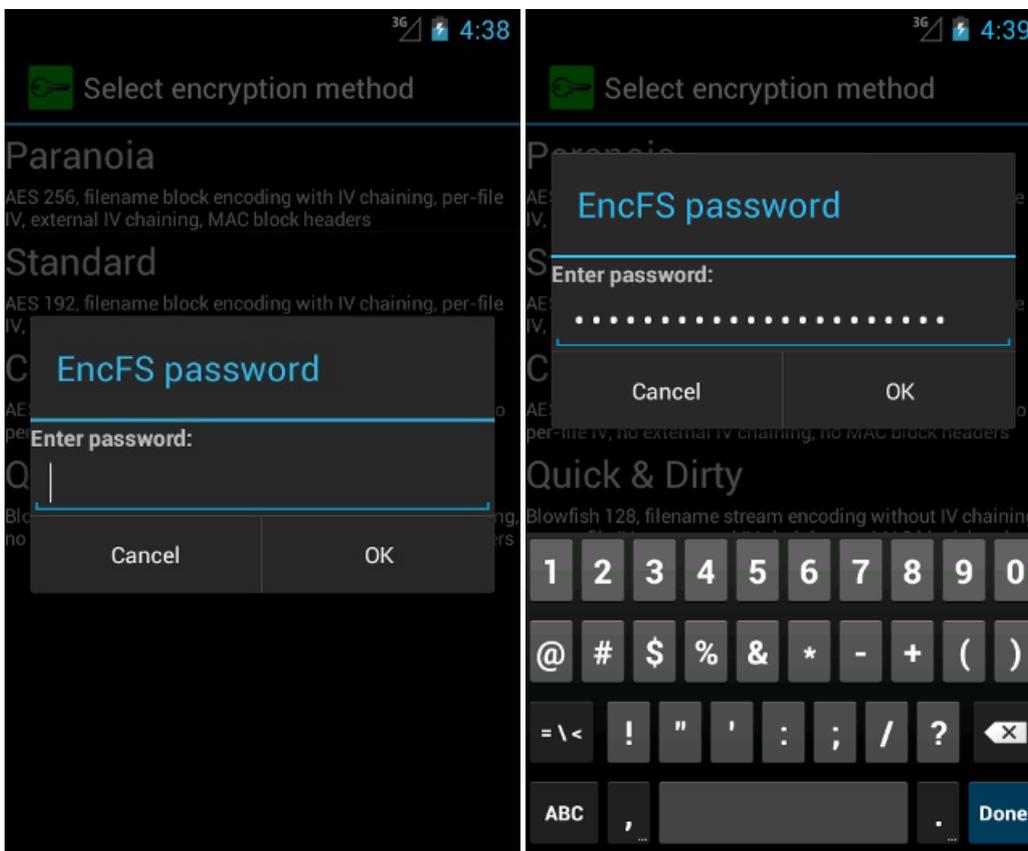
Graphiques 12 et 13 : Comment créer un nouveau dossier.

Étape 6. Un nouveau dossier est créé comme ci-dessous. **Cliquez** sur *Use current folder* (utiliser le dossier courant).



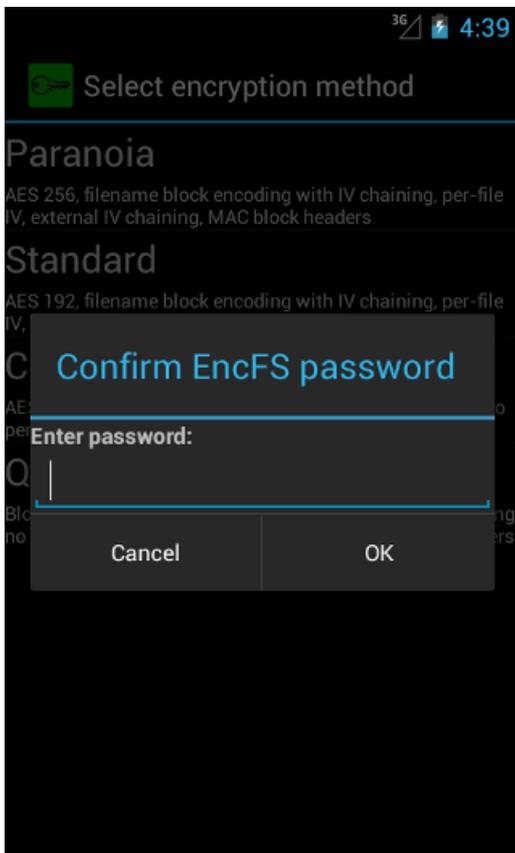
Graphiques 14 et 15 : Sélectionner un dossier.

Étape 7. Une fenêtre apparaîtra dans laquelle il vous sera demandé d'entrer un mot de passe. **Entrez** votre mot de passe comme montré ci-dessous.



Graphiques 16 et 17 : Entrer un mot de passe.

Étape 8. Confirmez votre mot de passe.

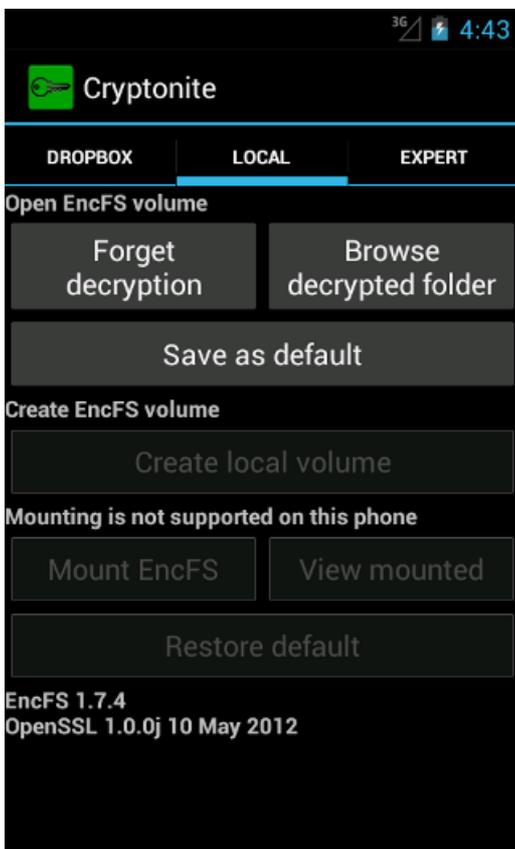


Graphique 18 : Confirmer son mot de passe

Félicitations ! Vous venez juste de créer un volume chiffré pour stocker des fichiers en toute sécurité.

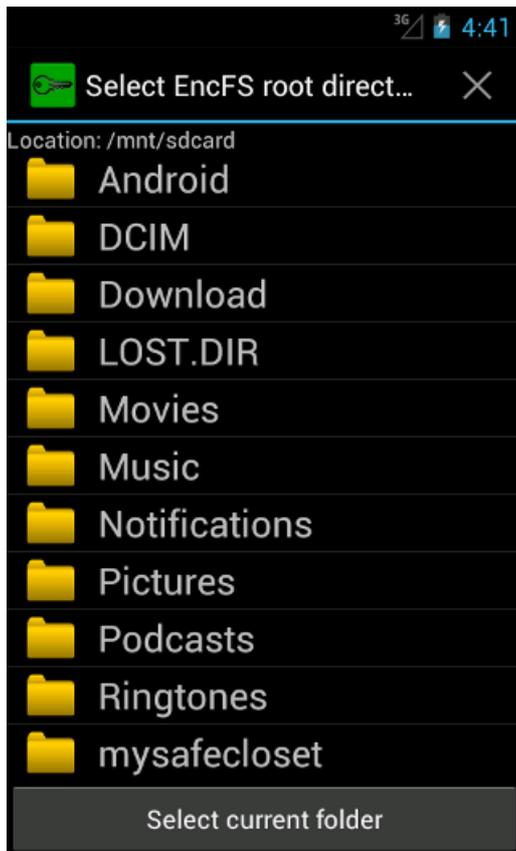
2.2 Comment télécharger des fichiers vers le répertoire Cryptonite

Étape 1. Appuyez sur *decrypt local folder* (déchiffrer le dossier local) et sélectionnez le dossier que vous aviez choisi auparavant.



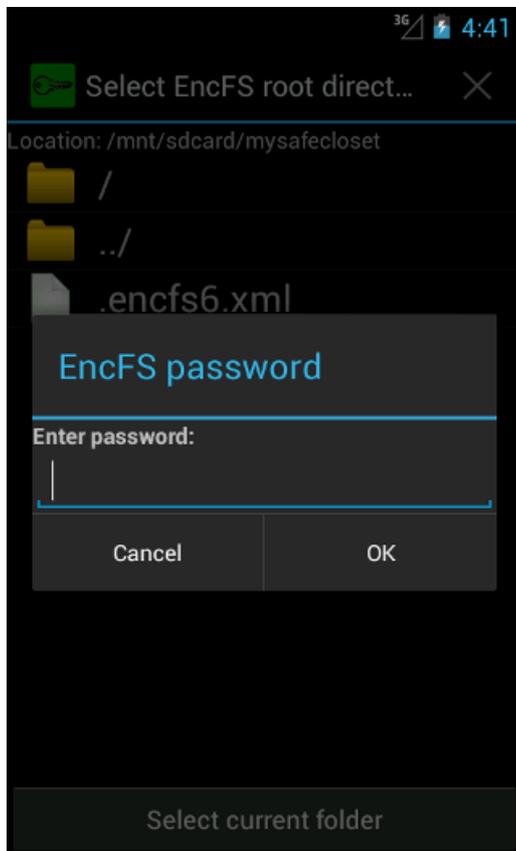
Graphique 19 : Options de déchiffrement.

Étape 2. Naviguez jusqu'au dossier que vous avez créé et **cliquez** sur *Select current folder* (sélectionner le dossier courant)



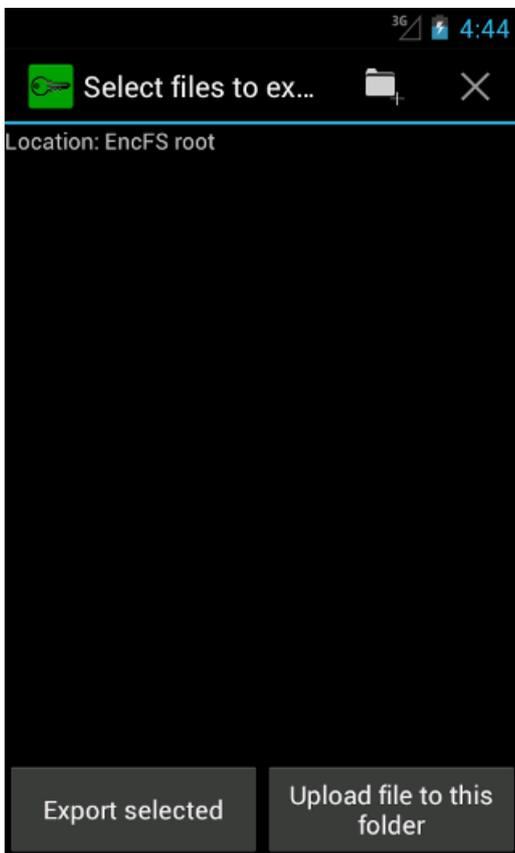
Graphique 20 : Sélectionner un dossier.

Étape 3. Entrez le mot de passe que vous avez créé pour accéder à ce dossier.



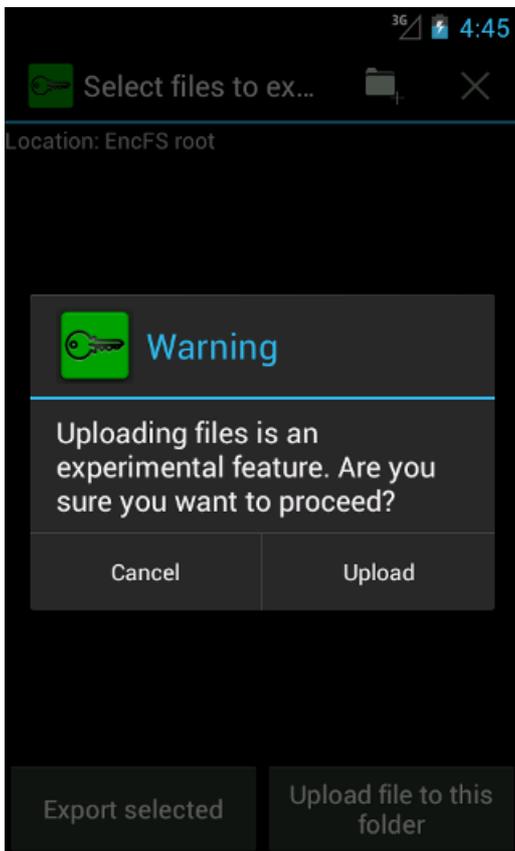
Graphique 21 : Entrer son mot de passe.

Étape 3. Appuyez sur *upload file to this folder* (télécharger le fichier vers ce dossier) pour y sauvegarder un ou plusieurs fichiers en toute sécurité.



Graphique 22 : Sélection du dossier.

Étape 4. Un message tel que ci-dessous apparaîtra.



Graphique 23 : Avertissement.

Étape 5. Ceci achevé, **appuyez** sur *forget decryption* (oublier le déchiffrement). **Cryptonite** supprimera alors le fichier temporaire utilisé pour l'opération précédente et le dossier sera fermé dans un état chiffré.

Conseil : Pour vérifier ce que vous venez de faire, **quittez Cryptonite** et naviguez avec votre explorateur de fichiers jusqu'au volume chiffré que vous venez de créer. Vous devriez y trouver deux fichiers : un fichier meta qui décrit le

chiffrement utilisé (mais pas le mot de passe, bien sûr) et un fichier qui contient votre fichier chiffré avec un nom de fichier plutôt erratique.

Note : Le fichier original se trouve encore à son emplacement original.

Note : Selon l'appareil que vous utilisez, vous pourriez également être en mesure de créer un volume local que vous pouvez monter. C'est d'autant plus simple depuis que vous pouvez y accéder dans son état déchiffré avec votre explorateur de fichiers ou toute autre application.

Gibberbot pour appareils Android

Short Description:

Gibberbot est une application libre et open source pour appareils Android, créée par le [Guardian Project](#) [16], qui vous permet d'organiser et de gérer différents comptes de messagerie instantanée (MI) en utilisant une seule interface. Il utilise un logiciel **Off-the-Record (OTR)** [17] qui assure des communications authentifiées et sécurisées entre des clients incluant **Gibberbot**, **ChatSecure**, **Jitsi**, et **Pidgin** [18]. **Gibberbot** peut également renforcer votre anonymat et protéger vos communications contre de nombreuses formes de surveillance sur Internet en vous connectant via **Orbot** [19], ce qui permet au trafic Internet de votre smartphone d'être acheminé via le **réseau Tor** [20].

Online Installation Instructions:

Télécharger Gibberbot

À partir du site web officiel

- *Lisez l'introduction courte des **guides pratiques*** [3]
- *Cliquez sur l'icône **Gibberbot** ci-dessous pour ouvrir <https://guardianproject.info/apps/>*
- *Défilez vers le bas jusqu'à ce qu'apparaisse l'icône **Gibberbot**, puis cliquez sur *Download app (télécharger l'application)*
- *Cliquez sur la touche d'installation dans Google play*
- *Une fois installée, cliquez sur Open (ouvrir) pour démarrer l'application*

À partir de Google Play (Android FOSS repository)

- *Vous pouvez également installer **Gibberbot** à partir de **Google Play*** [21]
- *Une fois installée, cliquez sur Ouvrir pour démarrer l'application*

Gibberbot:



[22]

Page d'accueil

- [Page d'accueil de Gibberbot](#) [23]
- [Site du développeur de Gibberbot](#) [24]

Matériel requis

- Android 1.6 ou plus récent

Version utilisée dans ce guide

- 0.0.9-RC4

Licence

- FOSS (GPLv3)

Lecture requise

- Livret pratique, chapitre **8. Préserver votre anonymat et contourner la censure sur Internet** [14]
- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** [9]
- Livret pratique, chapitre **11. Utiliser votre smartphone en sécurité (autant que possible...)** [10]

Niveau 1 : Débutant, **2** : **Moyen**, **3** : Intermédiaire, **4** : Expérimenté, **5** : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 30 minutes

Ce que vous obtenez en retour :

- La faculté de **chatter en sécurité et de façon anonyme**

1.1 Ce que vous devez savoir sur cet outil avant de commencer

- **Gibberbot** travaille avec Google, Facebook, certains serveurs Jabber ou XMPP.
- Les comptes de service de messagerie instantanée doivent être créés au préalable. Si vous souhaitez créer un compte **MI**, nous recommandons fortement **Google Talk**. Merci de consulter le chapitre **4.0 Comment créer un compte Google Talk** ^[25] pour plus d'informations et d'instructions.
- Des précautions particulières doivent être prises pour préserver l'anonymat lors de la création et de l'utilisation de services MI.

2. Comment installer et utiliser Gibberbot

Liste des sections:

- **2.0 Comment installer Gibberbot**
- **2.1 Comment configurer les paramètres de Gibberbot**
- **2.2 Comment utiliser Gibberbot**
- **2.3 Comment vérifier l'identité de votre partenaire**

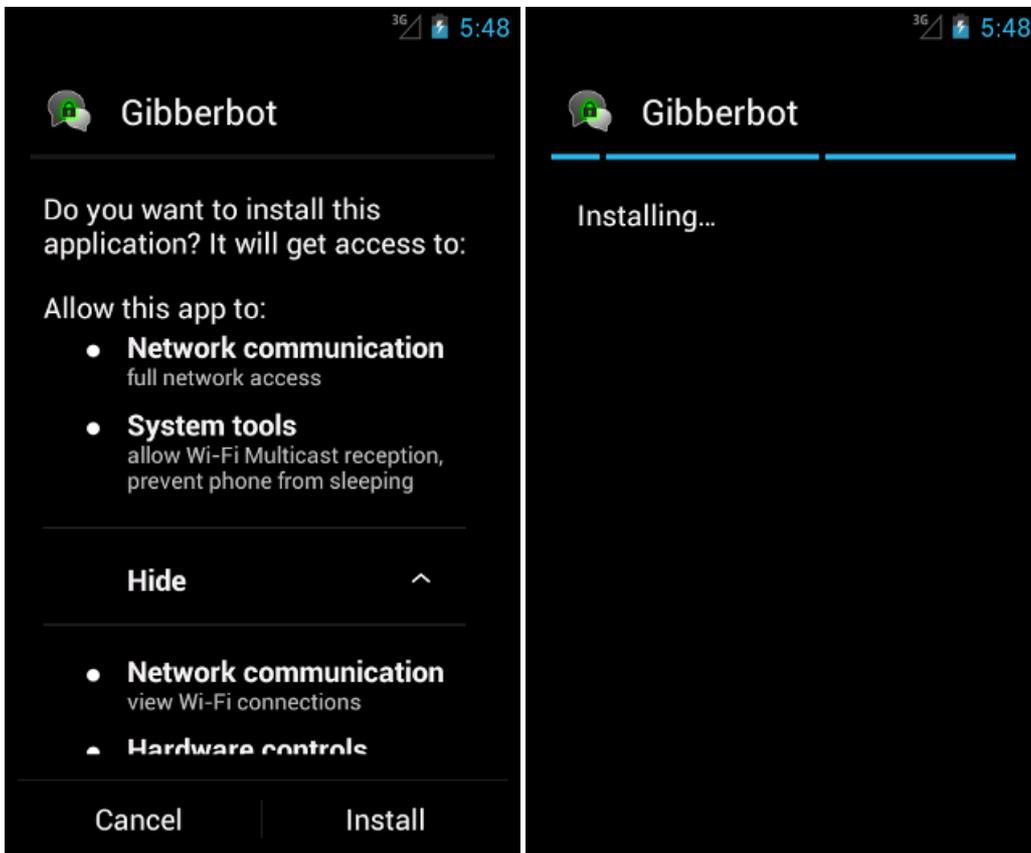
2.0 Comment installer *Gibberbot*

Étape 1. Téléchargez l'application à partir de la boutique [Google Play](https://play.google.com/s) ^[21]



Graphique 1 : Gibberbot dans la boutique Google Play.

Étape 2. Confirmez les autorisations requises par l'application et installez l'application en appuyant sur le bouton *Install*



Graphiques 2 et 3 : Autorisations et installation.

Étape 3. Appuyez sur *Open* (ouvrir) pour démarrer l'application une première fois.

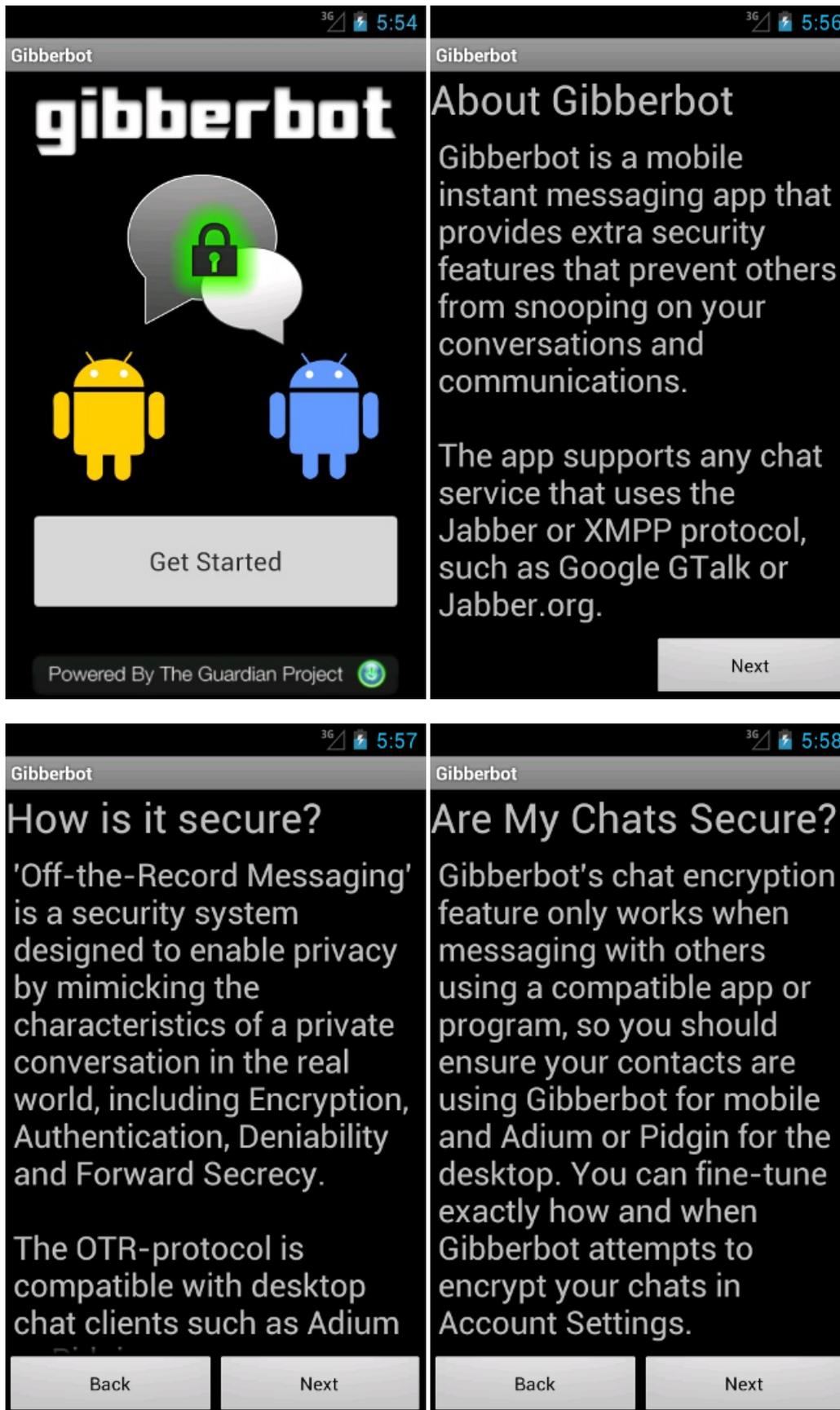
2.1 Comment configurer les paramètres de Gibberbot

Étape 1. Un menu déroulant de sélection des langues va apparaître. **Faites défiler** et **appuyez** sur la langue dans laquelle vous souhaitez utiliser **Gibberbot**.



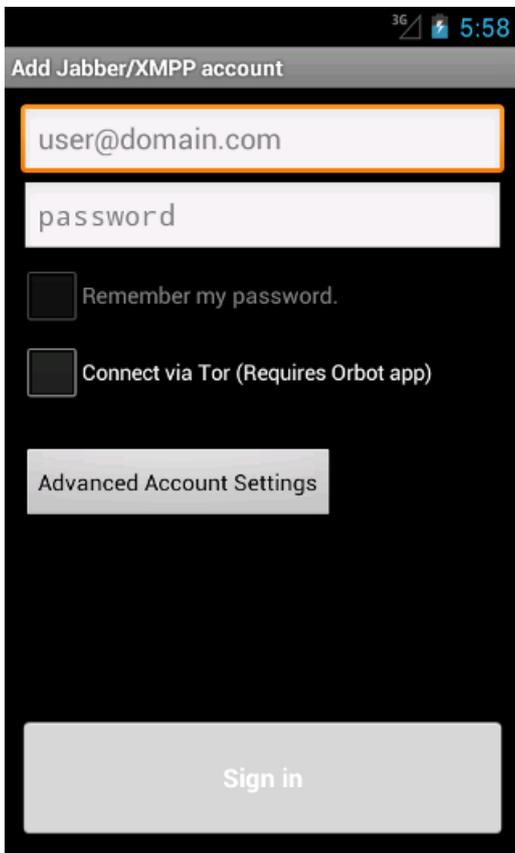
Graphique 4 : Options langue.

Étape 2. Appuyez sur *Démarrer* et *Suivant* 3 fois pour faire le tour des informations générales sur **Gibberbot**



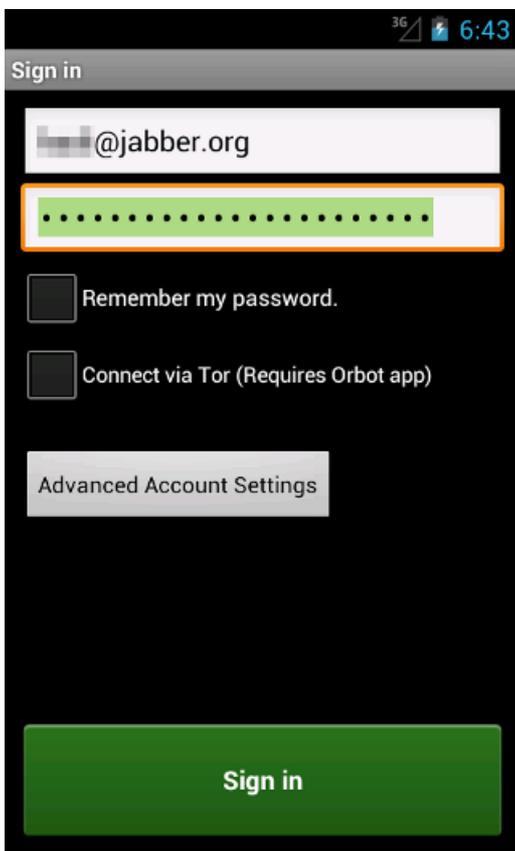
Graphiques 5, 6, 7, et 8 : Informations sur Gibberbot

Étape 3. La page de configuration du compte apparaît :



Graphique 9 : Page de configuration du compte.

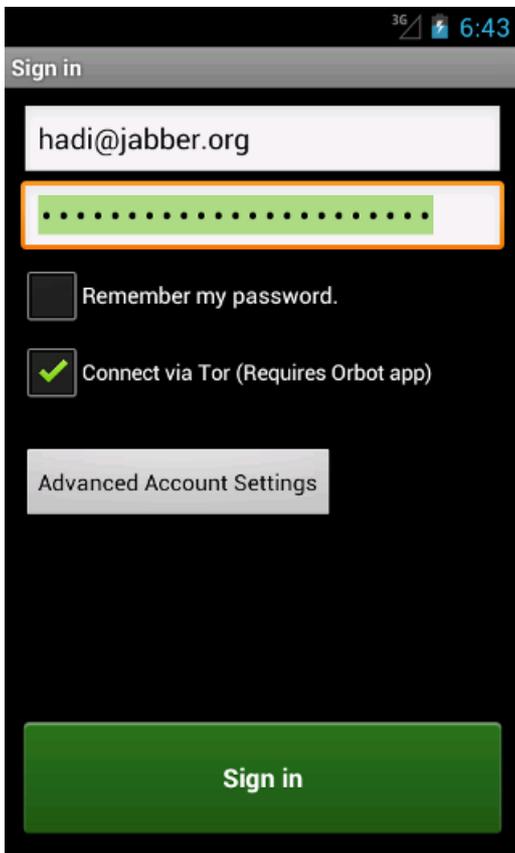
Étape 4. Ajoutez les données d'utilisateur et de serveur de la MI (par exemple "Joe@gmail.com"), puis **ajoutez** votre mot de passe associé.



Graphique 10 : Ajout des détails du compte

Note: Ne cochez **pas** l'option *Mémoriser mon mot de passe*, au cas où vous perdriez votre appareil.

Étape 5. Si vous avez installé et activé **Orbot** [26], **cochez** *Connecter avec Orbot* pour l'anonymat.

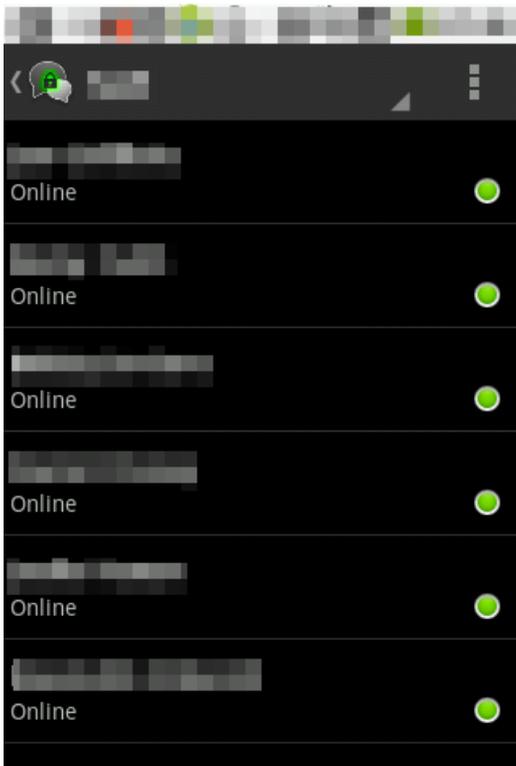


Graphique 11 : Connecter via Tor

Étape 6. Appuyez sur la touche *Se connecter*. Ceci fait, vous êtes prêt à utiliser **Gibberbot**.

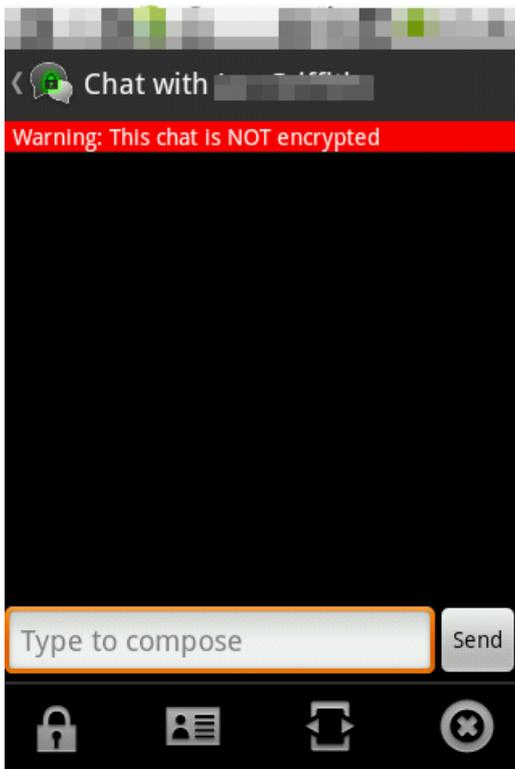
2.2 Comment utiliser Gibberbot

Étape 1. Lorsque vous ouvrez **Gibberbot** et accéder à votre compte, vous pouvez chatter avec les contacts de votre choix en **appuyant** sur leur nom.



Graphique 12 : Contacts en ligne

Étape 2. Quand le chat est lancé, le message *Attention : ce chat n'est PAS chiffré* vous alertera si vos communications ne sont pas sécurisées.

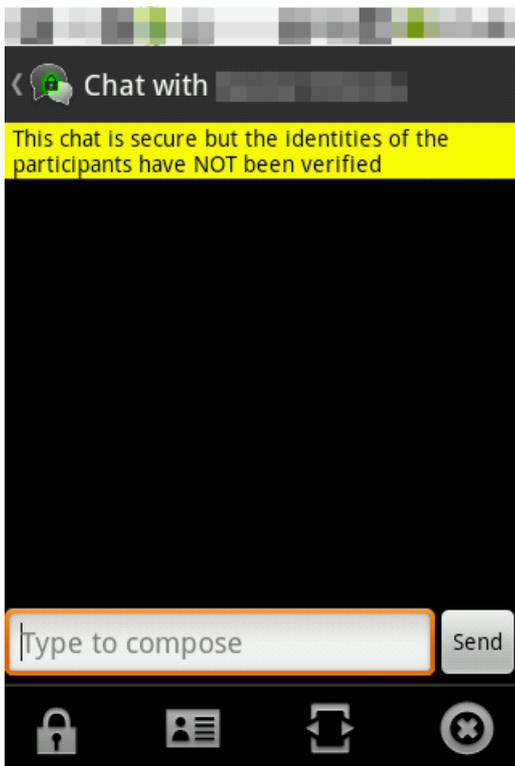


Graphique 13 : Ouvrir la fenêtre du chat

Étape 3. Vous pouvez démarrer une conversation chiffrée en appuyant sur



Étape 4. Si l'un de vos contacts utilise un client compatible avec OTR tel que Gibberbot, Pidgin [18] ou ChatSecure, le message d'avertissement indiquera en jaune : *Ce chat est sécurisé mais l'identité des participants n'a PAS été vérifiée.*



Graphique 14 : Chat sécurisé avec signatures numériques non vérifiées

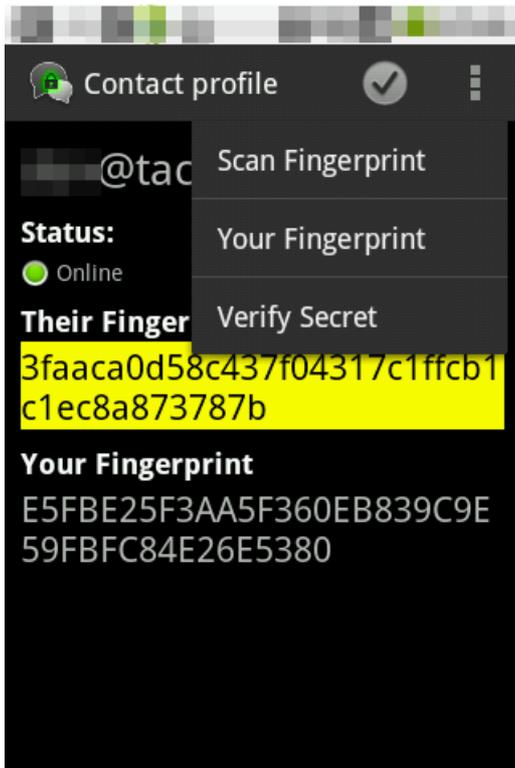
2.3 Comment vérifier l'identité de votre partenaire

Étape 1. Sélectionner l'option *Vérifier* dans le menu qui apparaît en appuyant sur



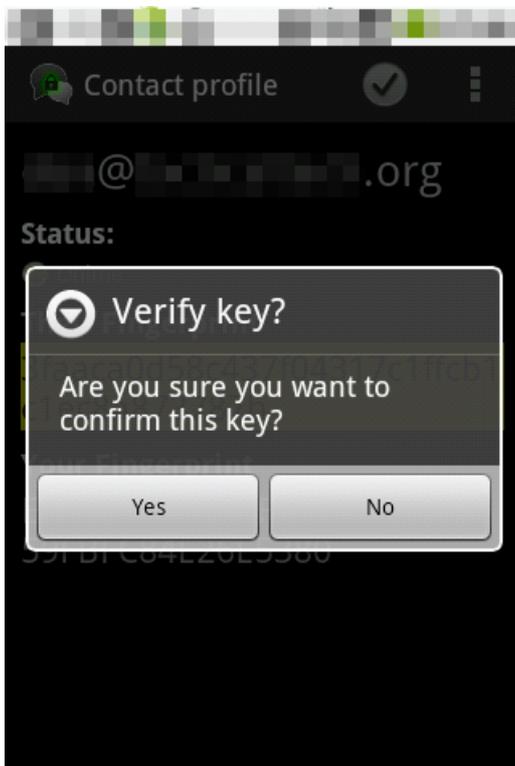
Étape 2. Comparez, soit en personne soit par un appel téléphonique ou un SMS, les deux valeurs d'empreinte présentées.

Étape 3. Si ces valeurs sont identiques, sélectionnez l'option *Vérifier secret* dans le menu comme ci-dessous.



Graphique 15 : Options de vérification

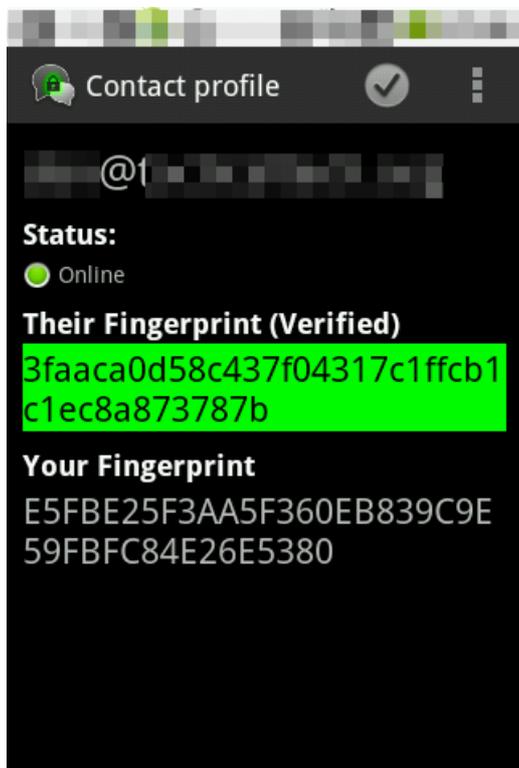
Étape 4. Une fenêtre va s'afficher comme ci-dessous, **cliquez** sur *OK* après vous être assuré que la personne à la signature numérique est bien la personne avec laquelle vous souhaitez parler.



Graphique 16 : Confirmer la vérification de la clé

Étape 5. Reprenez votre chat grâce à la touche *Retour*

Étape 6. Une fois l'identité vérifiée, le message en vert *Ce chat est sécurisé et vérifié* apparaîtra durant le chat.



Graphique 17 : Chat sécurisé vérifié

Étape 6. À partir du moment où les empreintes digitales ont été vérifiées, toutes les sessions suivantes de chat avec ce contact seront sécurisées et afficheront ce même message en vert.

Note: Si vous chattez avec **Gibberbot** et Pidgin ou d'autres clients de messagerie instantanée sécurisés à partir du même compte, en même temps, des problèmes liés aux différentes signatures numériques peuvent survenir. Assurez-vous que tous les autres clients sont bien déconnectés avant de vous reconnecter avec Gibberbot.

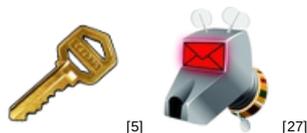
K9 et APG pour appareils Android

Online Installation Instructions:

Télécharger K-9 et APG

- Lisez l'introduction courte des **guides pratiques** ^[3]
- Cliquez sur l'icône **APG** ci-dessous pour ouvrir <http://www.thialfihar.org/projects/apg/>
- Défilez vers le bas jusqu'à download (téléchargement). Vous pouvez alors scanner le code QR de téléchargement et installation.
- Cliquez sur l'icône **K-9** ci-dessous pour ouvrir <https://code.google.com/p/k9mail/>
- Défilez vers le bas jusqu'aux téléchargements et télécharger l'apk.
- Déplacez le fichier apk que vous avez téléchargé sur votre appareil Android pour l'installer.

APG: K-9:



Android Privacy Guard (APG) est une application Android libre et open source, créée par [Thialfihar](#) ^[1], qui vous permet de chiffrer et déchiffrer des fichiers individuels ou des courriels. Il propose une implémentation OpenPGP pour Android. Toutefois, toutes les fonctions d'OpenPGP ne sont pas encore en état de marche. Son système de clés publique/privée vous permet de chiffrer, déchiffrer et signer des fichiers et des messages. Vous pouvez également l'utiliser pour chiffrer des fichiers individuels avec un chiffrement asymétrique, sécurisant les fichiers au moyen d'un mot de passe.

K-9 est un client de messagerie libre et open source pour Android, qui s'intègre parfaitement à **Android Privacy Guard**.

L'utilisation de ces deux outils permet le chiffrement et le déchiffrement facile de messages électroniques OpenPGP.

Page d'accueil

- [Page d'accueil de K-9](#) ^[28]

Matériel requis

- Android 1.5 ou plus récent
- APG doit être installée avant **K-9**

Version utilisée dans ce guide

- 4.011

Licence

- FOSS (Apache 2.0)

Lecture requise

- Livret pratique, chapitre **7. Préserver la confidentialité de vos communications sur Internet** ^[8]
- En particulier, vous devriez bien connaître la section **7.4. Principes de sécurité avancée** ^[11]
- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** ^[29]
- Livret pratique, chapitre **11. Utiliser votre smartphone en sécurité (autant que possible...)** ^[10]

Niveau 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : **Expérimenté**, 5 : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 30 minutes

Ce que vous obtenez en retour :

- La faculté d'utiliser une **messaging chiffrée sur votre Android**

1.1 Ce que vous devez savoir avant de commencer à utiliser cet outil

- Vous devez posséder un compte de messagerie électronique.
- Vous avez besoin d'une paire de clés OpenPGP ainsi que des clés publiques des personnes avec lesquelles vous souhaitez communiquer.
- Vous devez bien connaître le concept de chiffrement à clés publique/privée.
- Vous devez être en ligne lors de l'installation et de l'utilisation de **K-9**.
- En raison de la nature du stockage de données sur smartphones, la clé privée que vous générez ou importez ne peut pas être supprimée de façon sûre.

2. Comment installer et utiliser K-9 avec APG

Liste des sections:

- **2.0 Comment installer K-9**
 - **2.1 Comment configurer K-9**
 - **2.2 Comment utiliser K-9 avec APG**
-

2.0 Comment installer K-9

Étape 1. Téléchargez l'application à partir de la boutique [Google Play](#) ^[30]

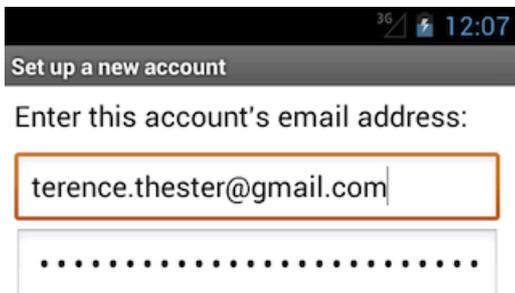
Étape 2. Installez l'application en appuyant sur la touche **Install**

Étape 3. Confirmez les autorisations requises par l'application et appuyez sur **Accept & download** (accepter & télécharger)

Étape 4. Appuyez sur *Open* (ouvrir) pour démarrer l'application une première fois

2.1 Comment configurer K-9

Étape 1. Lorsque vous démarrez **K-9**, il vous est demandé d'ouvrir un nouveau compte. **Entrez** alors votre adresse électronique et votre mot de passe.



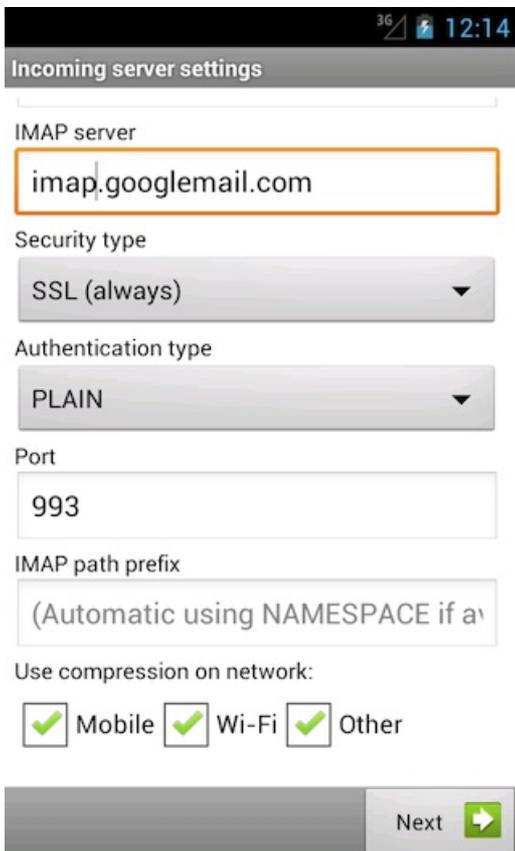
Graphique 1 : Entrer son adresse électronique

Étape 2. Sélectionnez le type de compte que vous avez (IMAP/POP/Exchange). En cas de doute, **vérifiez** le client de messagerie électronique sur votre ordinateur.



Graphique 2 : Options Compte de messagerie

Étape 3. Suivent maintenant les paramètres du serveur entrant. En cas de doute, reportez-vous au client de messagerie électronique sur votre ordinateur pour les réglages. **Assurez-vous** toujours que le *type de sécurité* est réglé soit sur *SSL* (*always - toujours*) ou *TLS* (*toujours*). Ne **jamais** utiliser l'option *none* (aucun).

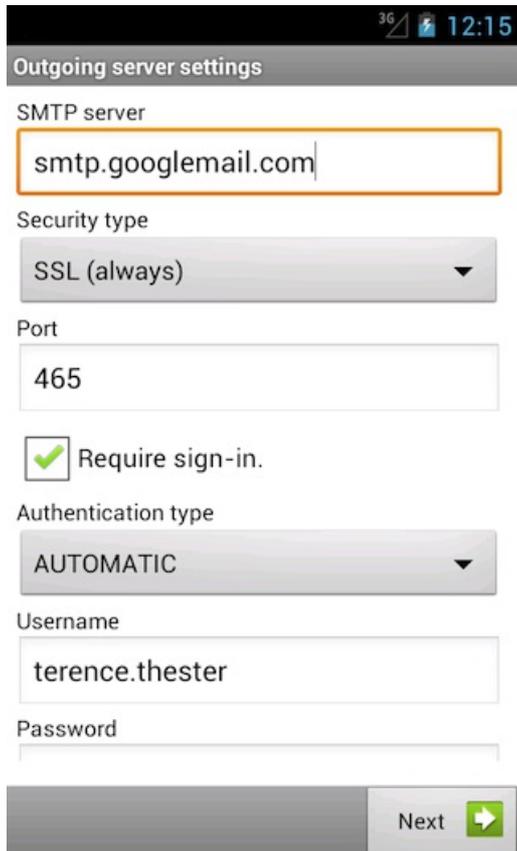


Graphique 3 : Paramètres du serveur entrant

Étape 4. K-9 va se connecter ensuite à votre serveur de messagerie électronique pour vérifier si vos paramètres fonctionnent. Il se peut qu'il affiche un avertissement sur le certificat de votre connexion sécurisée. *Ne l'ignorez pas!* C'est le seul moment où vous pouvez vérifier si le certificat appartient vraiment à votre serveur de messagerie. Si vous ignorez ceci, vous ne pouvez pas savoir avec certitude si vous n'êtes pas l'objet d'une *attaque de l'homme du milieu*, et vos

communications pourraient être interceptées. Vous verrez une signature numérique SHA-1 tout à la fin de l'avertissement. Vous devez alors soit **vérifier** sur votre ordinateur si le certificat installé de votre serveur de messagerie a la même signature numérique, soit trouver un moyen de vérifier le certificat de votre serveur de messagerie directement auprès de votre fournisseur.

Étape 5. K-9 vous demande de configurer vos paramètres de serveur sortant. À nouveau, **assurez-vous** que le *type de sécurité* est *SSL (always - toujours)* ou *TLS (toujours)*. Pour tous les autres paramètres, **vérifiez** le client de messagerie de votre ordinateur ou les paramètres de votre fournisseur de messagerie.



36 12:15

Outgoing server settings

SMTP server
smtp.googlemail.com

Security type
SSL (always)

Port
465

Require sign-in.

Authentication type
AUTOMATIC

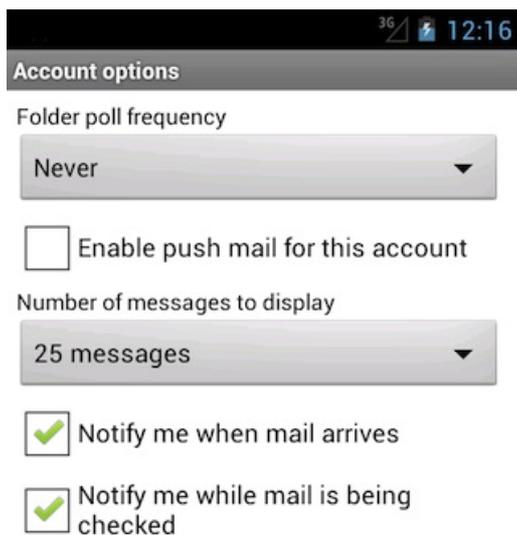
Username
terence.thester

Password

Next

Graphique 4 : Paramètres du serveur sortant

Étape 6. K-9 vous demande maintenant la fréquence avec laquelle vous souhaitez qu'il repère de nouveaux courriels. **Réglez** l'option sur *never* (jamais), ce qui signifie que vous vérifierez vous-même vos courriels.



36 12:16

Account options

Folder poll frequency
Never

Enable push mail for this account

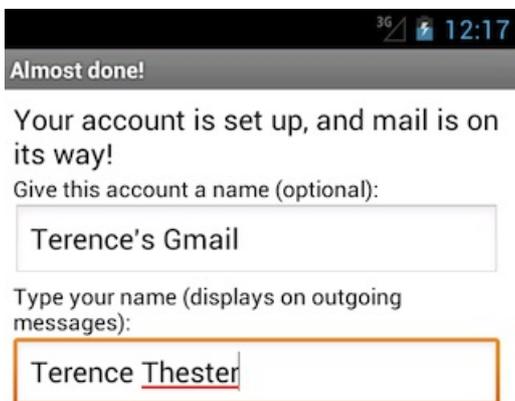
Number of messages to display
25 messages

Notify me when mail arrives

Notify me while mail is being checked

Graphique 5 : Fréquence de scrutation

Étape 7. Les derniers éléments d'information à fournir sont un surnom pour le compte de messagerie électronique qui sera affiché dans **K-9** et le nom que vous souhaitez voir apparaître dans tous les courriels sortants.



Graphique 6 : Options Nom du compte

Étape 8: Pour vous assurer que le compte fonctionne avec **K-9**, **envoyez-vous** à vous-même un courriel de votre ordinateur et téléchargez-le à partir du client **K-9**.



Nous vous recommandons d'utiliser **K-9** seulement en supplément du client de messagerie électronique de votre ordinateur. Il est donc important, lorsque vous téléchargez un courriel avec votre téléphone Android, que ce même courriel ne soit pas supprimé sur le serveur si vous souhaitez le recevoir plus tard également sur votre ordinateur. Par défaut, **K-9** est configuré ainsi, mais il se peut que souhaitez vérifier et en savoir plus sur les paramètres proposés dans les *comptes*. Pour cela, il suffit d'appuyer longtemps sur le compte que vous venez de créer et de sélectionner *Paramètres du compte* dans le menu. Vous pouvez ainsi également vérifier et régler les paramètres des options *réception* et *envoi de courriel*.

2.2 Comment utiliser K-9 avec APG

Avant de pouvoir envoyer et recevoir du courrier électronique chiffré, vous devez vous assurer que vous avez importé toutes vos clés OpenPGP dans APG. Pour ce faire, il vous faut copier toutes les clés de votre ordinateur vers votre téléphone.

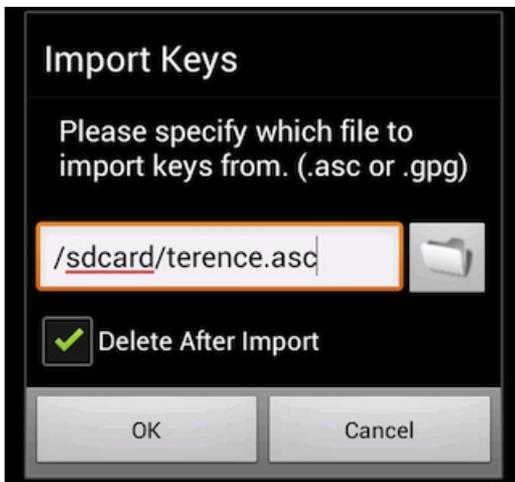
Une fois la copie effectuée, suivez les étapes suivantes pour importer vos clés dans APG.

Étape 1. Ouvrez APG.

Étape 2. Appuyez sur la touche *Menu* et **sélectionnez** *manage secret keys* (gestion des clés secrètes).



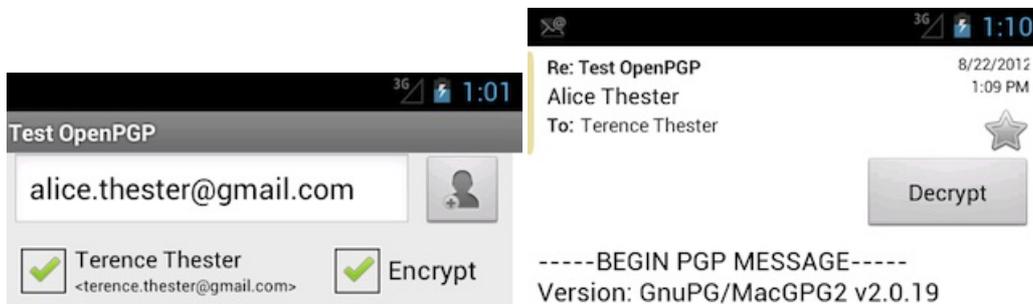
Étape 3. Appuyez sur la touche *Menu* à nouveau et sélectionnez *Import keys* (import des clés) . Entrez l'emplacement où vous avez stocké votre paire de clé privée et appuyez sur *OK*. Une fois l'import effectué, répétez les étapes ci-dessus et importez vos clés publiques à partir du menu *manage public keys* (gestion des clés publiques).



Graphique 7 : Options Gestion des clés

Étape 4. Pour importer vos clés publiques, **réitérez** les étapes 2 et 3, en prenant soin de sélectionner *manage public keys* (gestion des clés publiques) à l'étape 2.

Étape 5. Une fois que votre (vos) paire(s) de clés et votre collection de clés publiques ont été importées vers APG, **K-9** vous donnera la possibilité de *signer* et *chiffrer* des messages lors de l'écriture de courriels, ou bien de déchiffrer du courrier chiffré que vous avez reçu.



KeePassDroid pour appareils Android

Short Description:

KeePassDroid est un outil de gestion de mot de passe pour votre appareil Android sûr et facile à utiliser.

Online Installation Instructions:

Télécharger KeePassDroid

À partir du site web officiel

- Lisez l'introduction courte des **guides pratiques** ^[3]
- Cliquez sur l'icône **KeePassDroid** ci-dessous pour ouvrir <http://www.KEEPASS.INFO/download.html>
- Défilez vers le bas pour télécharger KeePassDroid
- Transférez le fichier apk que vous avez téléchargé vers votre appareil Android pour l'installer

À partir de Google Play

- Vous pouvez également installer **KeePassDroid** à partir de **Google Play** ^[31]
- Une fois installée, cliquez sur Open (ouvrir) pour démarrer l'application

KeePassDroid :



^[32]

Page d'accueil

- [KeePassDroid](#) ^[33]

Matériel requis

- Android 1.5 ou plus récent

Version utilisée dans ce guide

- 1.9.8

Licence

- Freeware GPL-V2

Lecture requise

- Livret pratique, chapitre **3. Créer et sauvegarder des mots de passe sûrs** ^[7]
- Guides pratiques **KeePass - Stockage de mots de passe** ^[34]

Temps nécessaire pour commencer à utiliser cet outil : 10 minutes

Ce que vous obtenez en retour:

- La faculté de sauvegarder tous vos mots de passe dans une base de données pratique et sûre
- La faculté de créer et de stocker plusieurs mots de passe forts sans pour autant devoir les mémoriser
- La faculté de partager vos fichiers de base de données de mots de passe KeePass entre votre appareil mobile et votre ordinateur

1.1 Ce que vous devez savoir sur cet outil avant de commencer

KeePassDroid est un outil puissant et facile à utiliser qui vous permet de stocker et gérer vos mots de passe dans une base de données hautement sécurisée. Vous pouvez copier votre fichier actuel de base de données KeePass de votre ordinateur vers l'application **KeePassDroid** de votre appareil mobile. **Notez** : Avant de copier et d'ouvrir votre base de données de mots de passe sur votre appareil mobile, sachez que la sûreté et la protection dispensées par votre appareil mobile n'égalent pas celles de votre ordinateur. La base de données est protégée par un 'mot de passe maître' que vous créez. Ce mot de passe est également utilisé pour chiffrer la totalité du contenu de la base de données. Vous pouvez stocker des mots de passe déjà existants dans **KeePassDroid** ou lui en faire générer un nouveau. **KeePassDroid** ne nécessite aucune configuration préalable et ne comporte pas d'instructions d'installation spécifiques. Il est prêt quand vous l'êtes !

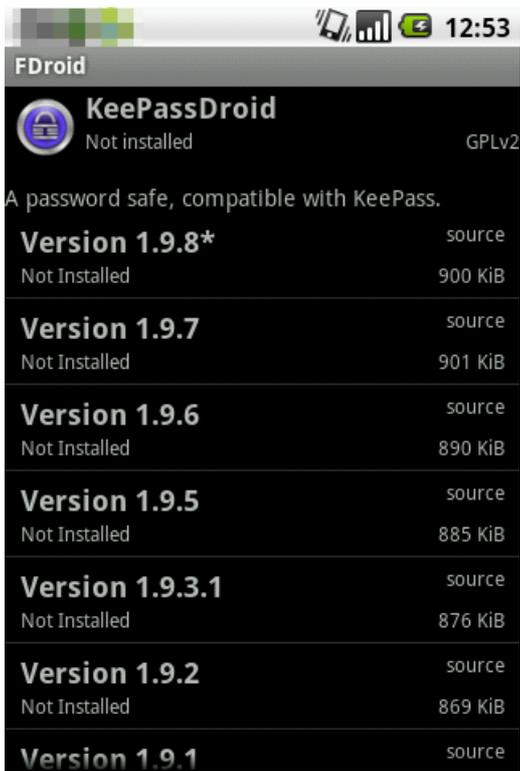
2. Comment installer et utiliser KeePassDroid

Liste des sections :

- [2.0 Comment installer KeePassDroid](#)
 - [2.1 Comment créer une nouvelle base de données de mots de passe](#)
 - [2.2 Comment ajouter un groupe et une entrée](#)
 - [2.3 Comment modifier une entrée](#)
 - [2.4 Comment générer des mots de passe aléatoires](#)
 - [2.5 Comment verrouiller la base de données KeePassDroid](#)
 - [2.6 Comment créer une sauvegarde du fichier de la base de mots de passe](#)
 - [2.7 Comment réinitialiser votre mot de passe maître](#)
-

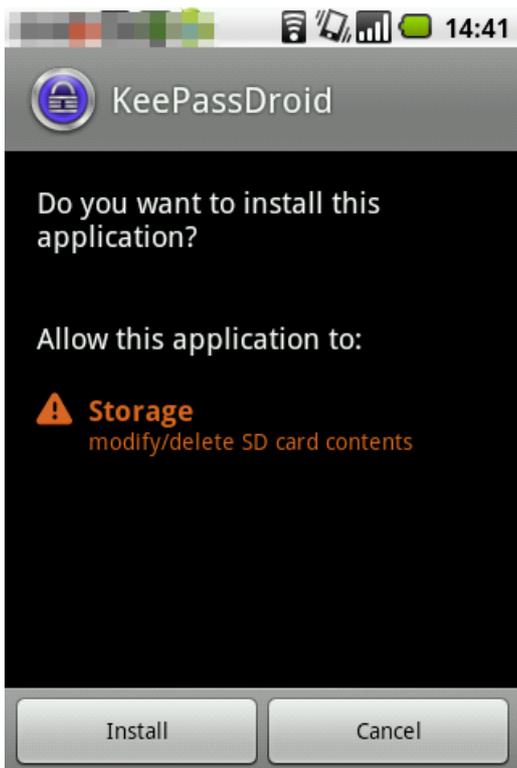
2.0 Comment installer KeePassDroid

Étape 1. Téléchargez l'application à partir de [Google Play](#) ^[31].



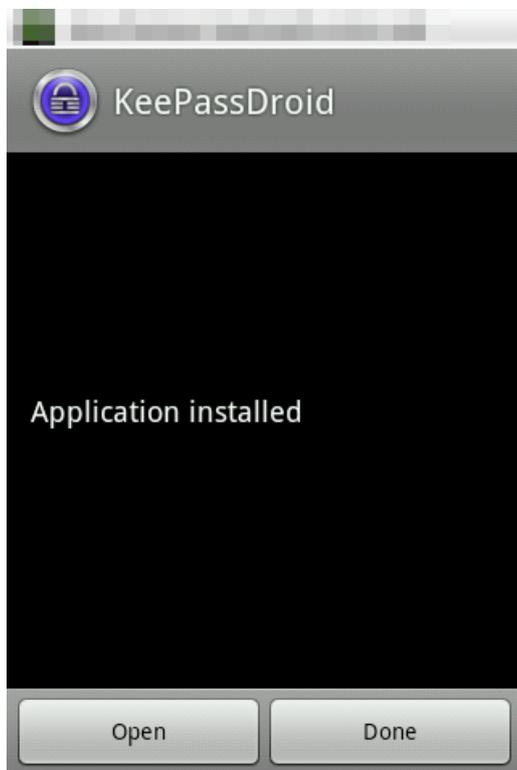
Graphique 1 : Versions de KeyPassDroid

Étape 2. Une fois le téléchargement effectué, cliquez sur **Package installer** (installeur du paquetage, puis **cliquez** sur **Install** (installer).



Graphique 2 : Autorisations nécessaires pour KeyPassDroid

Étape 3. Cliquez sur **Open** (ouvrir) comme montré dans la capture d'écran ci-dessous pour activer **KeePassDroid**.



Graphique 3 : Écran de l'application installée.

2.1 Comment créer une nouvelle base de données de mots de passe

Dans les sections qui suivent, vous allez apprendre à créer un mot de passe maître, sauvegarder votre base de données nouvellement créée, générer un mot de passe aléatoire pour un programme particulier et créer une copie de sauvegarde de la base de données.

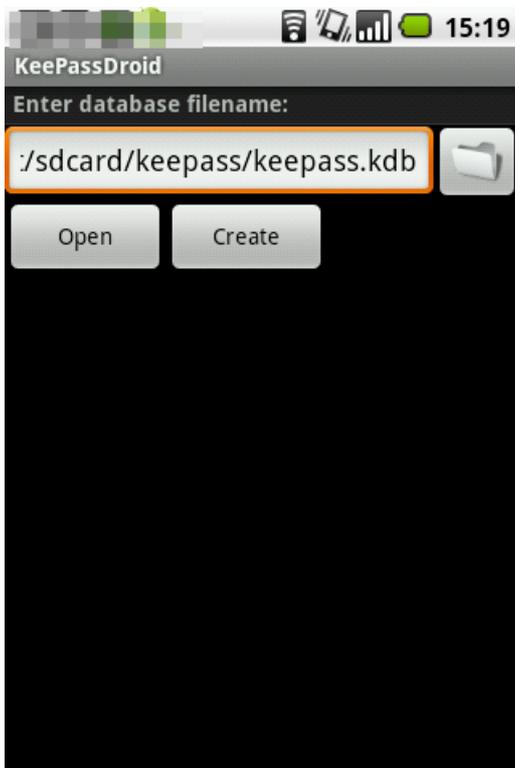
Pour ouvrir **KeePassDroid**, il vous faut cliquer sur l'icône de l'application.



Créer une nouvelle base de données de mots de passe implique deux étapes : vous devez déterminer un mot de passe maître unique et complexe, que vous allez utiliser pour verrouiller et déverrouiller votre base de données de mots de passe. Vous devez ensuite sauvegarder cette base de données de mots de passe.

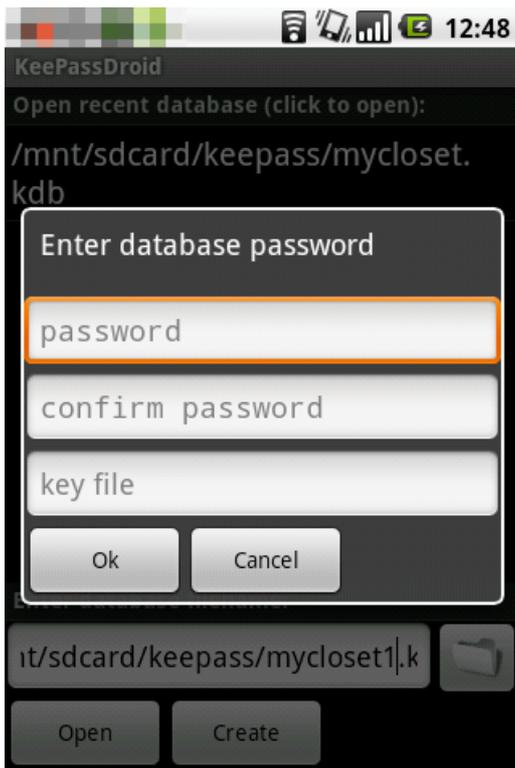
Pour créer une nouvelle base de données de mots de passe, suivez les étapes suivantes :

Étape 1. Pour créer une nouvelle base de données de mots de passe, **cliquez** sur *create* (créer).



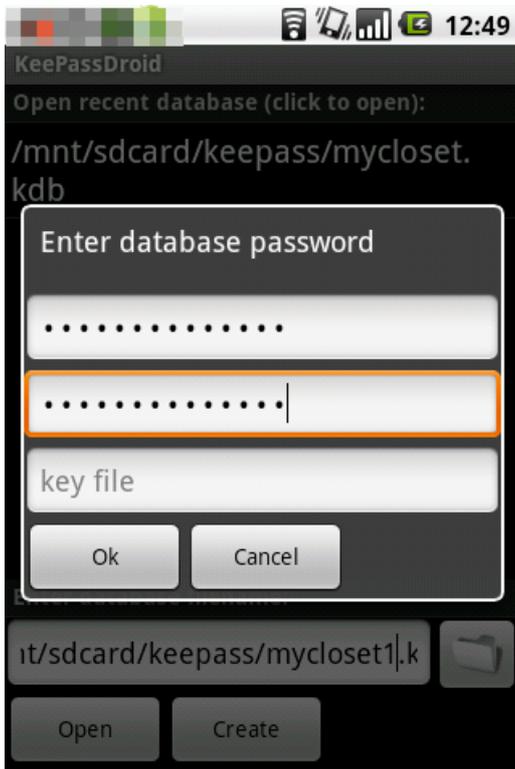
Graphique 4: Écran d'ouverture/création de la base de données.

L'écran *Enter database password* (Entrer le mot de passe de la base de données) sera activé comme ci-dessous:



Graphique 5 : Écran Entrer le mot de passe de la base de données.

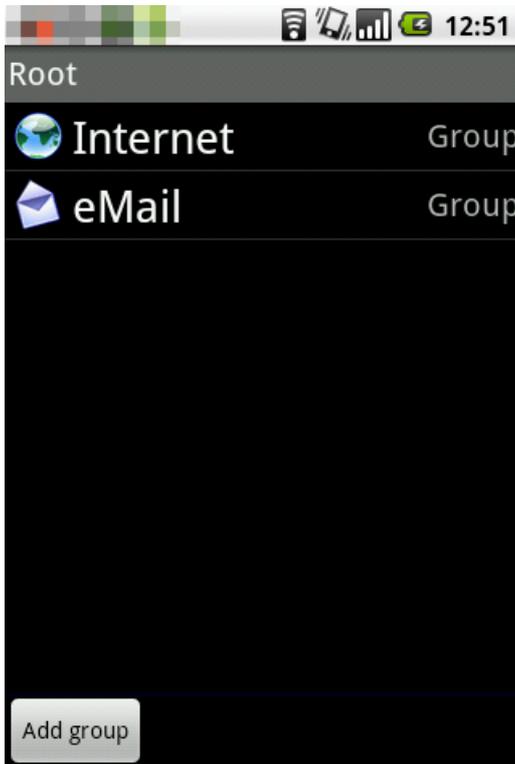
Étape 2. Tapez le mot de passe maître que vous avez inventé dans les champs *password* (mot de passe) et *confirm password* (confirmer le mot de passe), comme indiqué ci-dessous:



Graphique 6 : Entrer un mot de passe

Conseil: Assurez-vous d'avoir bien créé un mot de passe maître fort. Consultez [3. Créer et sauvegarder des mots de passe sûrs](#) [7] pour plus d'informations à ce sujet.

Étape 3. Cliquez sur **OK** pour activer l'écran suivant



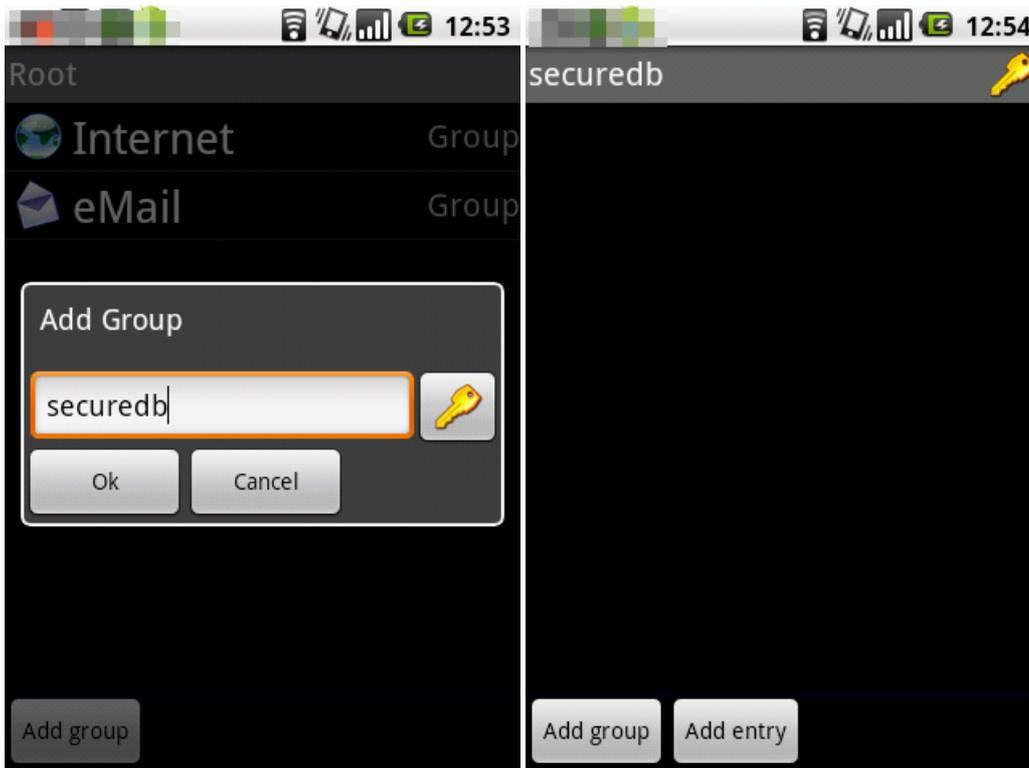
Graphique 7 : Écran d'accueil de KeePassDroid

Félicitations ! Vous venez de créer une base de données de mots de passe sécurisée. Vous pouvez maintenant commencer à y déposer tous vos mots de passe actuels et futurs.

Note: Vous pouvez également copier les fichiers de base de données **KeePass** existants de votre ordinateur vers votre appareil Android, puis les ouvrir avec **KeePassDroid**.

2.2. Comment ajouter un groupe et une entrée

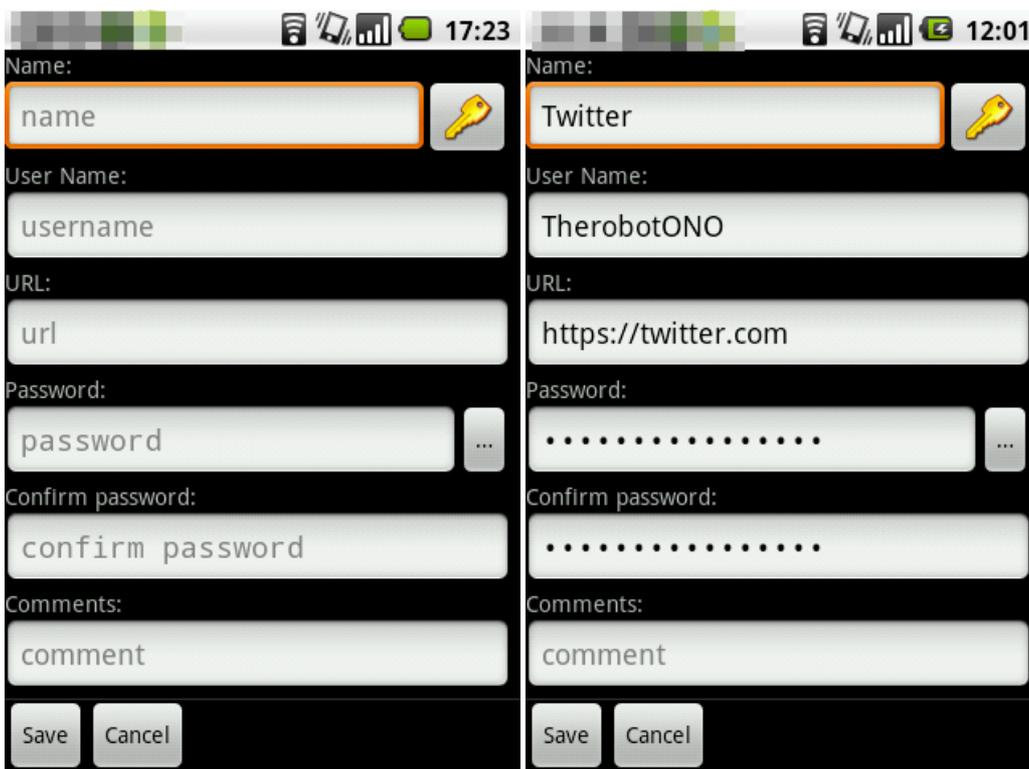
KeePassDroid conserve les entrées de mots de passe en groupes pour garder votre information organisée, les groupes par défaut sont **Email** et **Internet**, mais vous pouvez créer votre propre groupe en **cliquant** sur *Add Group* (ajouter un groupe) et en tapant le nom du groupe, puis sur **OK** pour activer l'écran suivant :



Graphiques 8 et 9 : Ajouter un nouveau groupe

L'écran **Add entry** (ajouter une entrée) vous permet d'ajouter des informations de compte, des mots de passe et autres détails importants dans votre base de données nouvellement créée. Dans l'exemple qui suit, vous allez ajouter des entrées pour stocker les mots de passe et noms d'utilisateur pour d'autres sites web et comptes de messagerie.

Étape 1. Cliquez sur *Add Entry* (ajouter une entrée) pour activer l'écran *Add Entry* comme suit :



Graphiques 10 et 11 : Ajouter une entrée de mot de passe.

Note: L'écran *Ajouter une entrée* présente plusieurs champs à compléter. Aucun de ces champs n'est obligatoire ; l'information fournie ici est à utiliser à votre guise. Elle peut s'avérer utile si vous recherchez une entrée particulière.

Ces différentes zones de textes vous sont brièvement expliquées ci-dessous :

Name (nom) : Un nom pour spécifier l'entrée du mot de passe. Par exemple, votre mot de passe gmail.

Username (nom d'utilisateur) : Le nom d'utilisateur associé à l'entrée du mot de passe. Par exemple, securitybox@gmail.com

URL : Le site Internet associé à l'entrée du mot de passe. Par exemple, https://mail.google.com

Password (mot de passe) : Cette fonction génère un mot de passe aléatoire lorsque l'écran *Add an entry* (ajouter une entrée) est activé. Vous pouvez utiliser cette fonction si vous souhaitez modifier un mot de passe existant par un mot de passe généré par KeePassDroid. Comme KeePassDroid s'en souviendra toujours pour vous, il ne vous est pas même nécessaire de voir le mot de passe. Un mot de passe généré de façon aléatoire est considéré comme fort (c'est à dire qu'il sera difficile à un intrus de le deviner ou de le cracker).

La section suivante décrit comment générer un mot de passe aléatoire. Vous pouvez bien sûr remplacer le mot de passe par défaut par un mot que vous avez créé vous-même. Par exemple, si vous créez une entrée pour un compte déjà existant, vous entrerez le mot de passe correct ici.

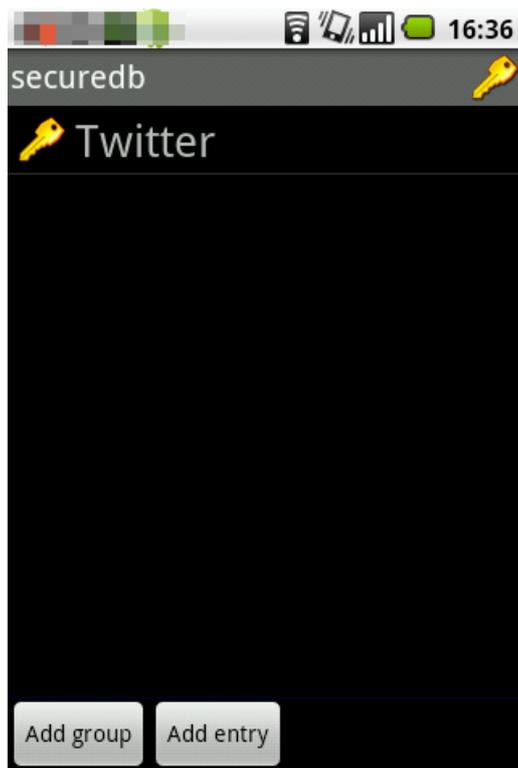
Confirm passwords (confirmer les mots de passe) : La confirmation du mot de passe.

Comments (commentaires) : C'est ici que vous inscrivez l'information descriptive ou générale du compte ou du site pour lequel vous stockez des informations. Par exemple : Paramètres du serveur de messagerie : *POP3 SSL, pop.gmail.com, Port 995; SMTP TLS, smtp.gmail.com, Port: 465*

Note : Le fait de créer ou de modifier les entrées de mot de passe dans **KeePassDroid** ne change en rien vos mots de passe courants ! Considérez **KeePassDroid** comme un carnet d'adresses électroniques sûr pour vos mots de passe. Il ne stocke que ce que vous y écrivez, rien d'autre.

Étape 2. Cliquez sur **save** pour sauvegarder vos modifications de l'écran d'ajout d'entrées.

Votre nouvelle entrée apparaît alors dans le groupe.



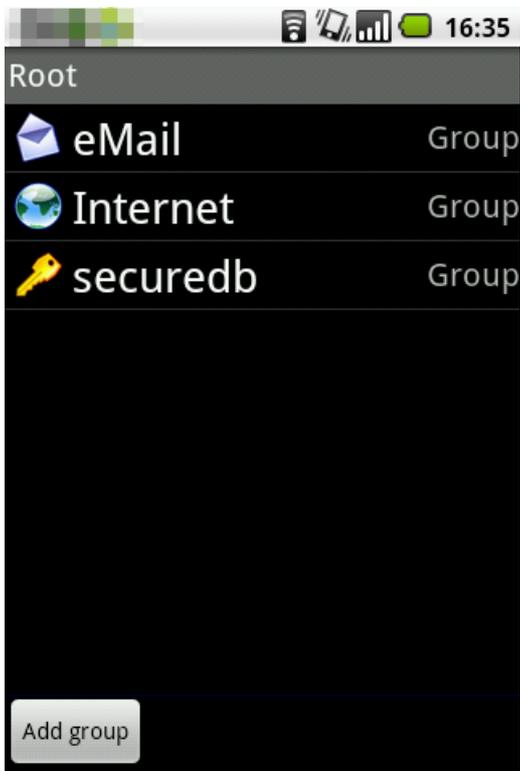
Graphique 12 : Nouvelle entrée apparaissant dans le groupe nouvellement créé.

2.3 Comment modifier une entrée

Vous pouvez modifier une entrée existante dans **KeePassDroid** à tout moment. Vous pouvez changer votre mot de passe (il est généralement conseillé de changer de mot de passe tous les trois ou six mois pour plus de sécurité) ou modifier d'autres détails stockés dans l'entrée du mot de passe.

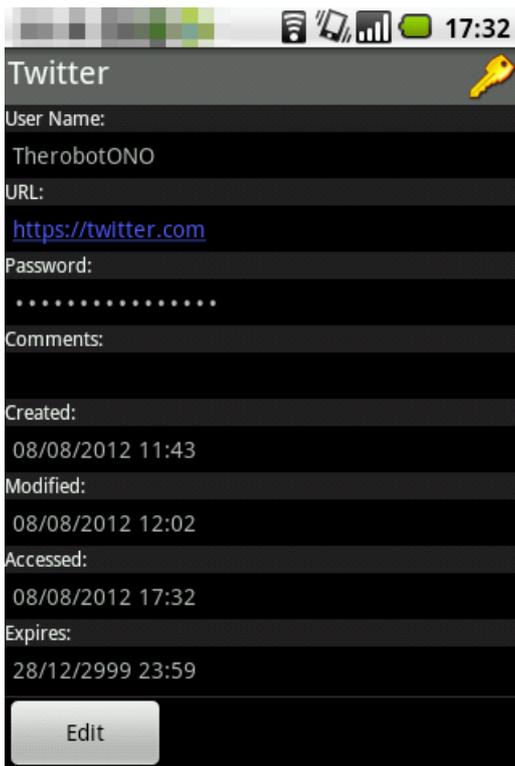
Pour modifier une entrée, effectuez les étapes suivantes :

Étape 1. Sélectionnez le *groupe* correct pour activer les entrées auxquelles il est associé.



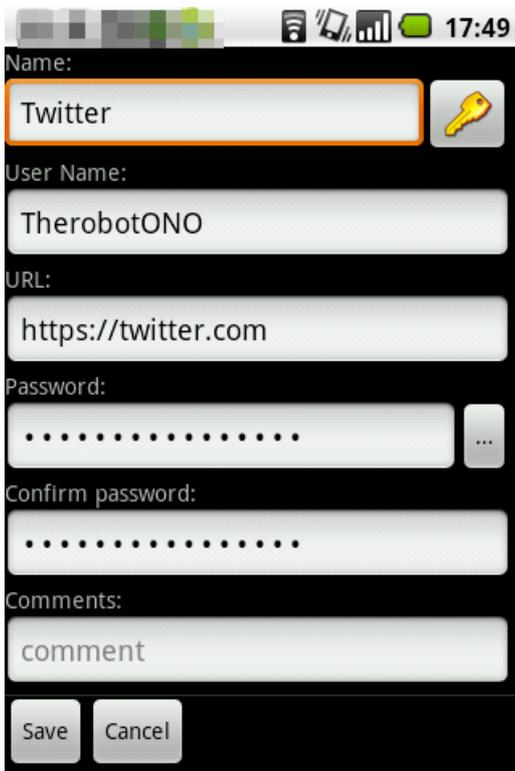
Graphique 13 : Liste de groupes.

Étape 2. Sélectionnez l'entrée correspondante, puis **cliquez** sur l'entrée sélectionnée pour activer la fenêtre suivante :



Graphique 14 : Aperçu de l'entrée.

Étape 3. Cliquez sur **Edit** (modifier), vous pouvez maintenant modifier l'information donnée. Ceci effectué, **cliquez** sur **save** (enregistrer) pour conserver les modifications nécessaires à l'information, y compris le mot de passe.



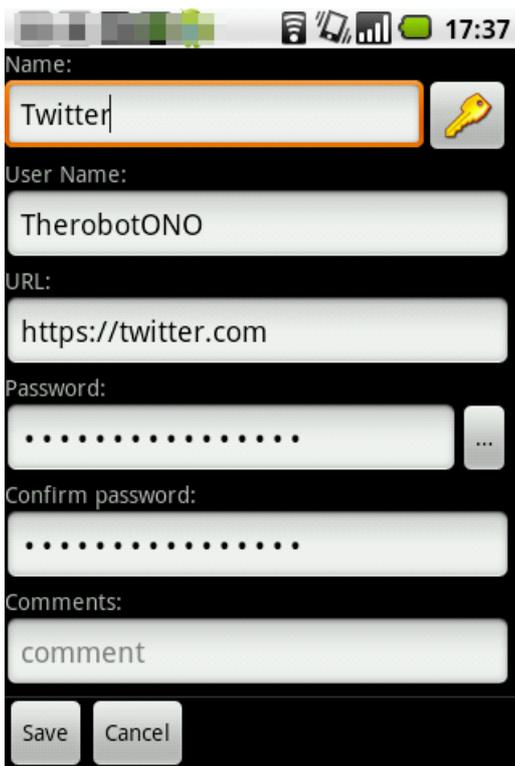
Graphique 15 : Modifier l'info.

Pour échanger un mot de passe existant (que vous avez créé vous-même au préalable) contre un mot de passe généré et recommandé par **KeePassDroid**, veuillez lire la section suivante.

2.4 Comment générer des mots de passe aléatoires

Les mots de passe aléatoires longs sont considérés comme forts dans le domaine de la sécurité. Leur caractère aléatoire est basé sur des principes mathématiques et ne peut pas être simplement 'deviné' par quelqu'un cherchant à cracker l'un de vos comptes. KeePass fournit un générateur de mots de passe facilitant cette procédure. Comme il vous a été montré ci-dessus, un mot de passe aléatoire est automatiquement généré lorsque vous ajoutez une entrée. Cette section décrit comment en générer un vous-même.

Note : Le *générateur de mots de passe* peut être activé à partir des écrans *Add Entry* (ajouter une entrée) et *Edit Entry* (modifier une entrée).



Graphique 16 : Info sur l'entrée de mots de passe.

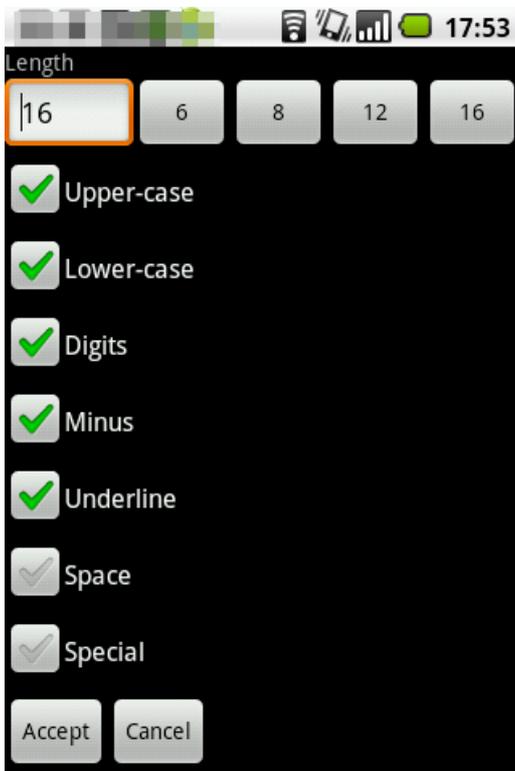
Étape 1. Cliquez la touche  soit à partir de l'écran *Add Entry* soit de l'écran *Edit Entry* pour activer l'écran du *générateur de mots de passe* comme suit :



Graphique 17 : Options pour la génération de mots de passe.

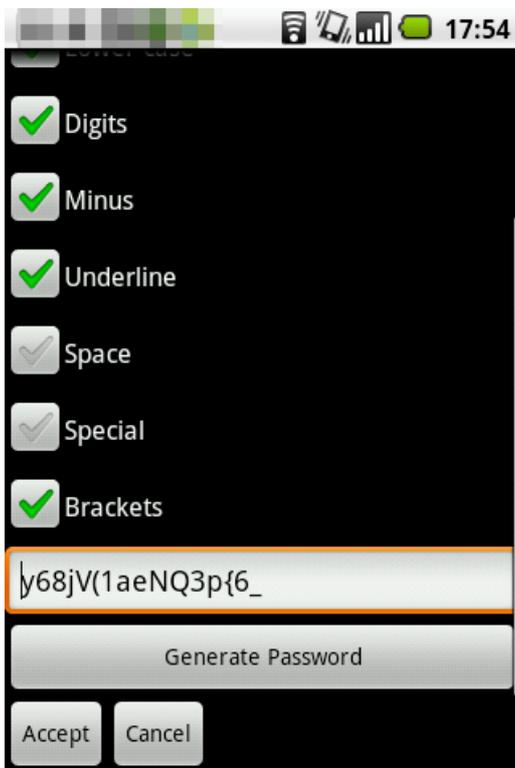
L'écran du générateur de mots de passe offre plusieurs critères quant à la création d'un mot de passe. Vous pouvez entre autres spécifier la longueur du mot de passe souhaité, le type de caractères que vous souhaitez utiliser. À titre exemplaire, nous allons sélectionner les options suivantes :

- **Longueur** d'au moins 16 caractères
- **Cochez** Upper-case Letter (lettre majuscule)
- **Cochez** Lower-case Letter (lettre minuscule)
- **Cochez** Digits (chiffres)
- **Cochez** Minus (tirets)
- **Cochez** Brackets (parenthèses)
- **Cochez** Underline (soulignages)



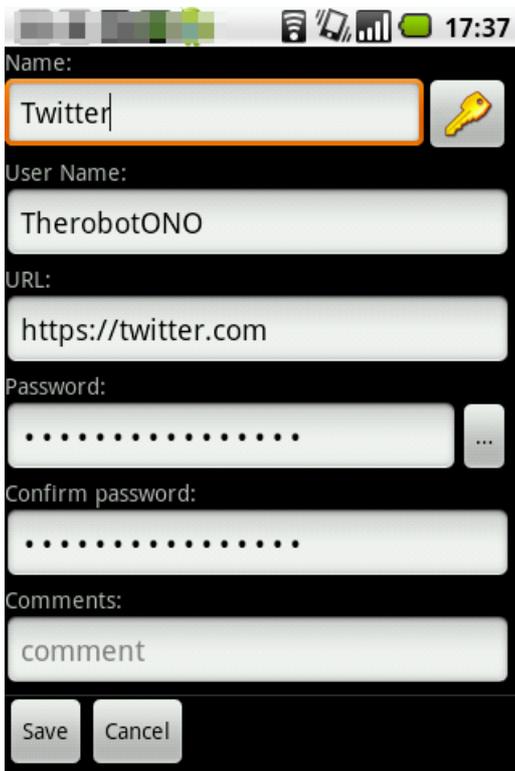
Graphique 18 : Options pour la création de mots de passe

Étape 2. Cliquez sur **Generate Password** pour démarrer la procédure. Une fois terminée, **KeePassDroid** affichera le mot de passe généré.



Graphique 19 : Exemple de mot de passe aléatoire.

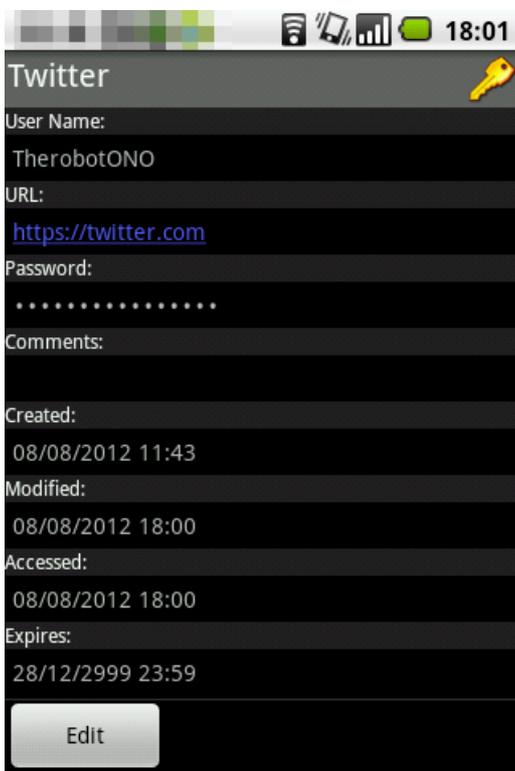
Étape 3. Cliquez sur **Accept** (accepter) pour activer l'écran suivant :



Graphique 20 : Informations de l'entrée

Note: Vous pouvez afficher le mot de passe généré en sélectionnant l'option correspondante dans le menu. Toutefois, comme nous l'avons évoqué ci-dessus, ceci constitue un risque quant à la sécurité. Par essence, il n'est pas nécessaire de voir le mot de passe généré. Nous revenons sur ce sujet dans la section **3.0 Comment utiliser les mots de passe** [35].

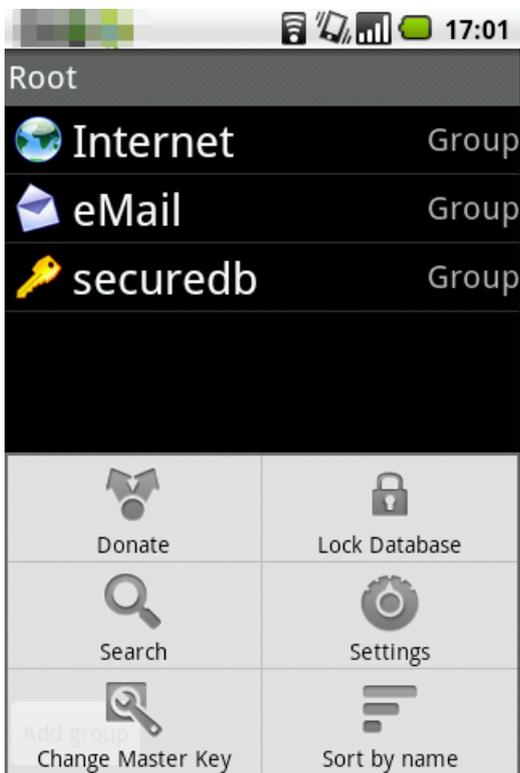
Étape 4. Cliquez sur Save (enregistrer) pour accepter le mot de passe et retourner à l'écran *Entry* (entrée), comme suit :



Graphique 21 : Écran d'entrée

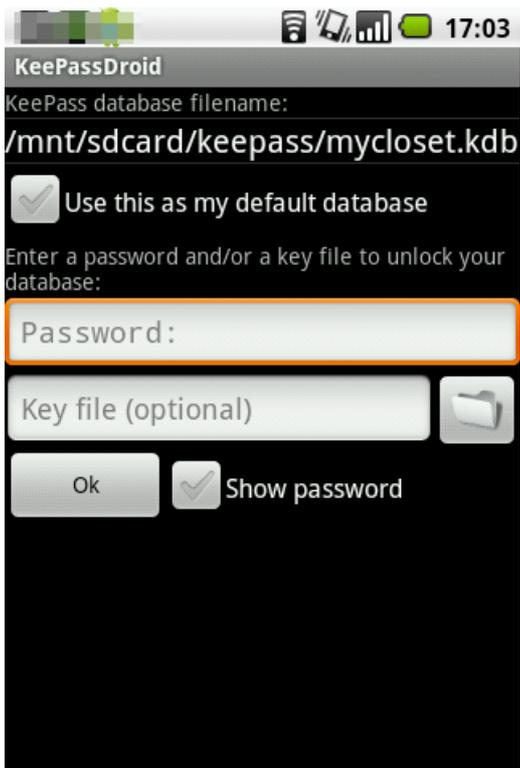
2.5 Comment verrouiller la base de données KeePassDroid

Étape 1. Cliquez sur la touche **Menu** pour activer l'écran suivant :



Graphique 22 : Options du menu

Étape 2. Cliquez sur *Lock Database* (verrouiller la base de données) pour désactiver la console **KeePassDroid** comme ci-dessous :



Graphique 23 : Base de données verrouillée

Il vous faut entrer votre mot de passe à nouveau pour accéder à votre base de données **KeePassDroid**.

2.6 Comment créer une sauvegarde du fichier de la base de mots de passe

Le fichier de la base de données **KeePassDroid** de votre téléphone Android est indiqué par son extension de fichier .kdb. Vous pouvez copier ce fichier sur votre ordinateur ou votre clé USB. Personne d'autre que vous ne sera en état d'ouvrir cette base de données sans le mot de passe maître.

Note : Pour ouvrir la base de données **KeePassDroid** que vous avez copiée depuis votre appareil Android sur votre ordinateur, vous devez vous assurer que le programme KeePass a bien été installé sur votre ordinateur ou que vous en

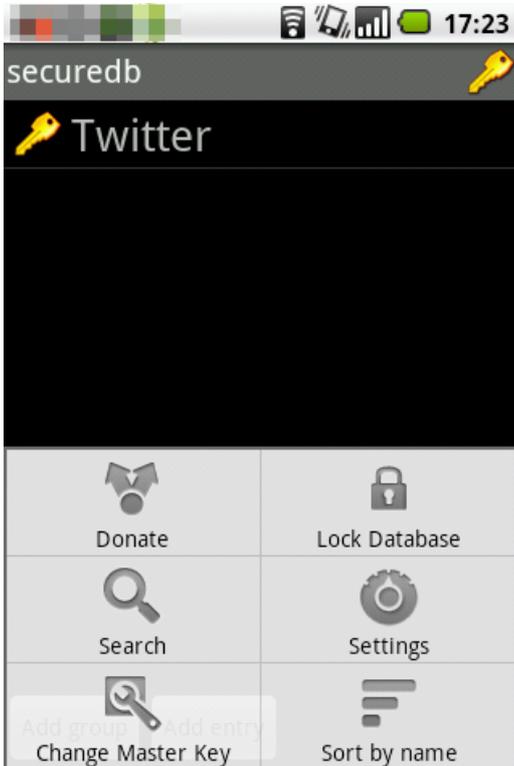
avez la version portable sur votre clé USB.

Consultez s'il vous plaît [Portable KeePass](#) ^[36] pour plus d'informations.

2.7 Comment réinitialiser votre mot de passe maître

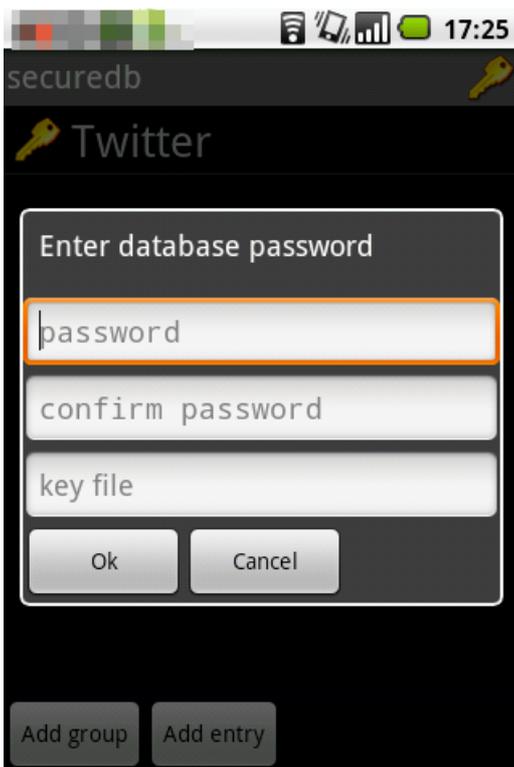
Vous pouvez modifier le mot de passe principal à tout moment. Ceci peut être effectué une fois que vous avez ouvert la base de données de mots de passe.

Étape 1. Sélectionnez la base de données et **cliquez** sur *Menu* pour activer l'écran suivant :



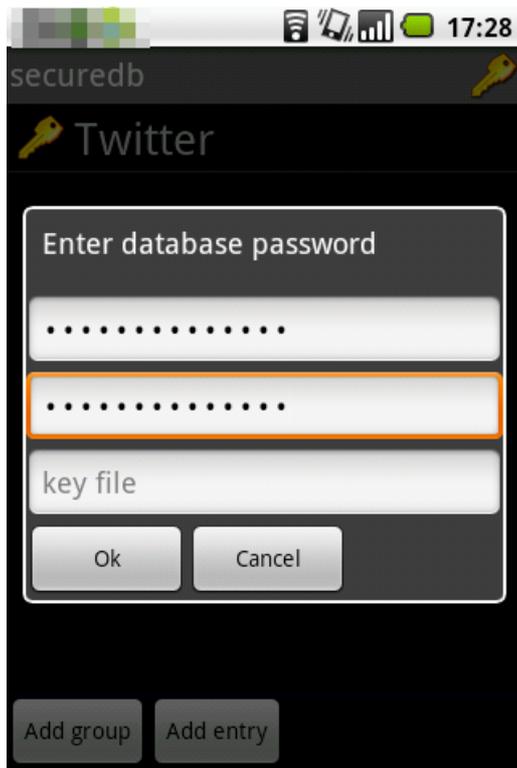
Graphique 24 : Options du menu

Étape 2. Cliquez sur **Change Master key** (modifier la clé principale) pour activer l'écran suivant :



Graphique 25 : Entrer un nouveau mot de passe.

Étape 3. Entrez votre mot de passe dans les champs **Password** (mot de passe) et **Confirm Password** (confirmer le mot de passe), puis **cliquez** sur OK.



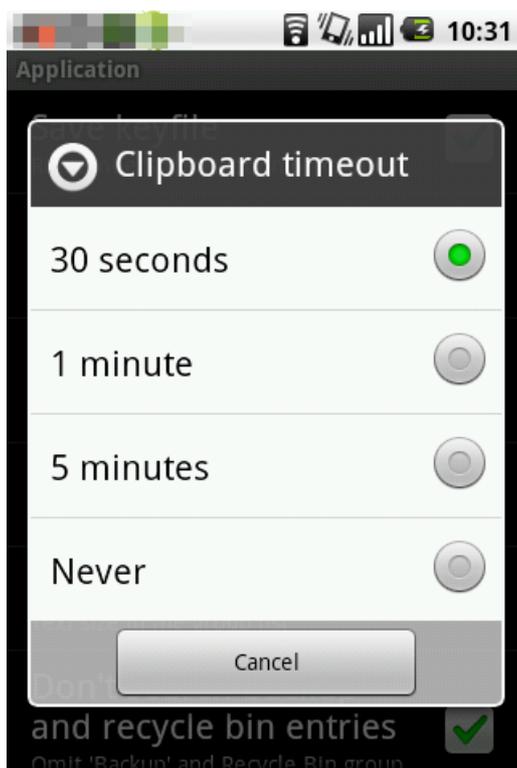
Graphique 26 : Entrer un nouveau mot de passe

3.0 Comment utiliser les mots de passe KeePassDroid

Puisqu'un mot de passe sécurisé est difficile à mémoriser, **KeePassDroid** vous permet de le copier depuis la base de données et de le coller directement dans le compte ou le site Internet qui le requiert.

Pour plus de sécurité, vous pouvez faire en sorte que le mot de passe copié dans le presse-papier n'y reste que **30 secondes**, **1 minute**, ou **5 minutes** de sorte que vous puissiez y coller le mot de passe correspondant sans devoir vous dépêcher avant qu'il ne soit automatiquement effacé du presse-papier.

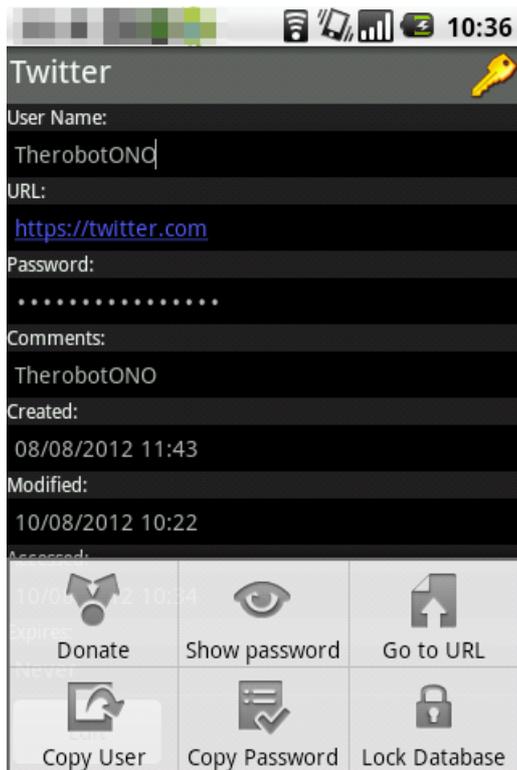
Vous pouvez voir ces options dans l'écran suivant en allant à : **Menu** > **Settings** (paramètres) > **Application** > **Clipboard timeout** (délai presse-papier)



Graphique 27 : Options délai du presse-papier.

Copier un mot de passe KeePassDroid

Étape 1. Cliquez dans **Menu** sur le mot de passe requis pour activer l'écran suivant :

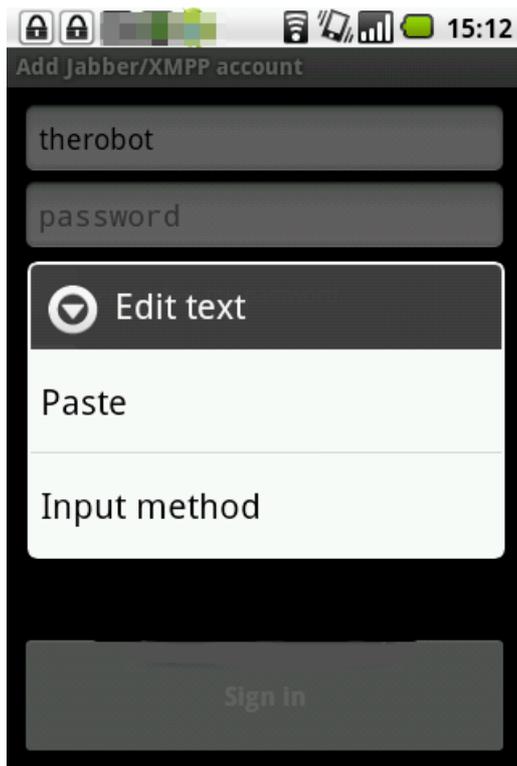


Graphique 28 : Options mots de passe



Étape 2. Sélectionnez **Copy Password**

Étape 3. Ouvrez le compte ou le site afférent et collez le mot de passe dans le champ correspondant en cliquant et maintenant le champ correspondant, puis sélectionnez *Paste* (coller) :



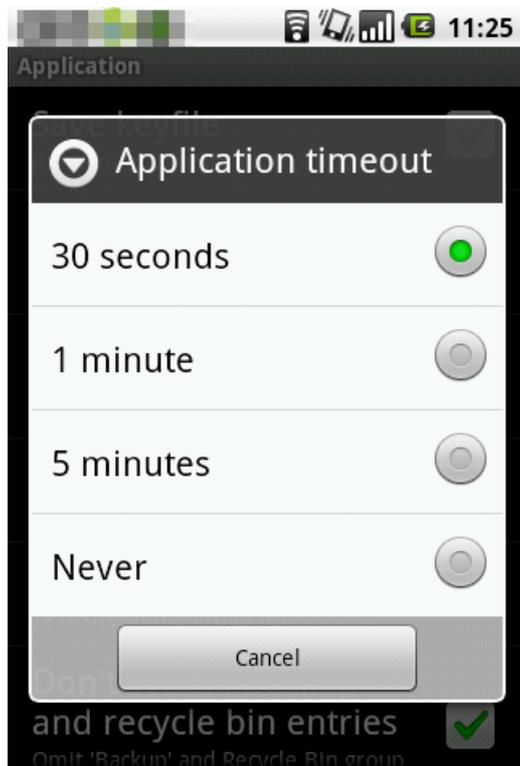
Graphique 29 : Options édition de texte

Note: Si vous utilisez **KeePassDroid** tout le temps, vous n'avez jamais réellement besoin de voir ou de connaître votre mot de passe. Les fonctions copier/coller suffisent à le déplacer depuis la base de données vers la fenêtre requise. Si vous utilisez la fonction *Générateur aléatoire* puis transférez le mot de passe vers le processus d'inscription d'un nouveau compte de messagerie, vous utiliserez un mot de passe que vous n'avez jamais vu. Et il continue de remplir sa tâche !

Verrouiller la base de données selon un délai

Il vous est également possible de verrouiller votre base de données lorsque l'application est restée inactive durant un temps déterminé. Ceci peut être affectué en allant à :

Menu > Settings (paramètres) > Application Cliquez sur Application timeout (délai application) pour activer ce qui suit :



Graphique 30 : Options Délai de l'application.

Sélectionnez le délai de verrouillage de votre base de données.

ObscuraCam pour appareils Android

Short Description:

ObscuraCam est une application photo libre pour appareils Android, créée par le [Guardian Project](#) ^[16], qui peut reconnaître et cacher les visages. Elle vous permet de brouiller ou effacer les visages de ceux que vous photographiez dans le but de protéger leur identité.

Online Installation Instructions:

Télécharger ObscuraCam

À partir du site web officiel

- Lisez l'introduction courte des **guides pratiques** ^[3]
- Cliquez sur l'icône **ObscuraCam** ci-dessous pour ouvrir <https://guardianproject.info/apps/>
- Défilez vers le bas jusqu'à ce que vous voyiez l'icône d'**ObscuraCam**, cliquez ensuite sur **Download App** (télécharger l'application)
- Cliquez sur la touche **Install** (installer) dans Google Play
- Une fois installée, cliquez sur open (ouvrir) pour démarrer l'application

À partir de Google Play

- Vous pouvez également installer **ObscuraCam** à partir de **Google Play** ^[37]
- Une fois installée, cliquez sur open (ouvrir) pour démarrer l'application

ObscuraCam :



[22]

Page d'accueil

- [Page d'accueil d'ObscuraCam](#) [38]
- [Site du développeur d'ObscuraCam](#) [39]

Téléphone requis

- Android

Version utilisée dans ce guide

- 2.0-RC2b

Licence

- FOSS (GPLv3)

Lecture requise

- Livret pratique, chapitre [9. Utiliser votre téléphone mobile en sécurité \(autant que possible...\)](#) [9]
- Livret pratique, chapitre [11. Utiliser votre smartphone en sécurité \(autant que possible...\)](#) [10]

Niveau : 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : Expérimenté, 5: Avancé

Temps nécessaire pour commencer à utiliser cet outil : 20 minutes

Ce que vous obtenez en retour :

- La faculté de **cache**r les visages dans les photos prises avec votre appareil Android
- Un moyen simple de **partager** ou **sauvegarder** ces photos « masquées »

1.1 Ce que vous devez savoir sur cet outil avant de commencer

- Le système de reconnaissance faciale d'**ObscuraCam** ne fonctionne pas toujours, il vous est toutefois toujours possible de facilement sélectionner et masquer les visages manuellement.
- Dans certaines versions du système d'exploitation Android, l'option de *suppression du fichier multimédia d'origine* ne fonctionne pas. si vous comptez sur cette option, assurez-vous s'il vous plaît qu'aucune photo **ObscuraCam** (avec des visages visibles !) ne se trouve dans votre appareil.
- Si vous utiliser **ObscuraCam** pour envoyer des photos à vous-même ou à quelqu'un d'autre, sachez que l'outil **ne** fournit **pas** de protection supplémentaire (telle que le chiffrement de bout en bout) de la photo en transit.

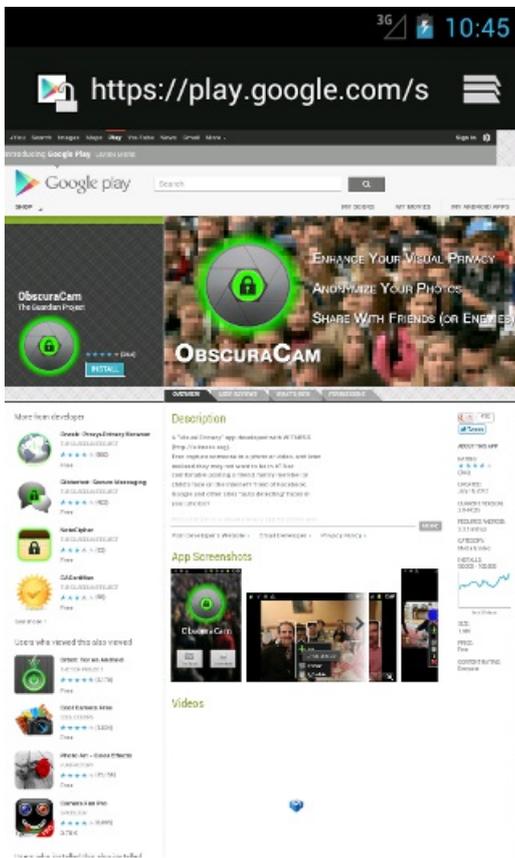
2. Comment installer et utiliser ObscuraCam

Liste des sections:

- [2.0 Comment installer ObscuraCam](#)
- [2.1 Prendre des photos avec ObscuraCam](#)
- [2.2 Masquer les visages dans des photos déjà existantes](#)
- [2.3 Modifier le mode « flou »](#)
- [2.4 Partager des photos](#)
- [2.5 Supprimer les fichiers multimédia d'origine](#)

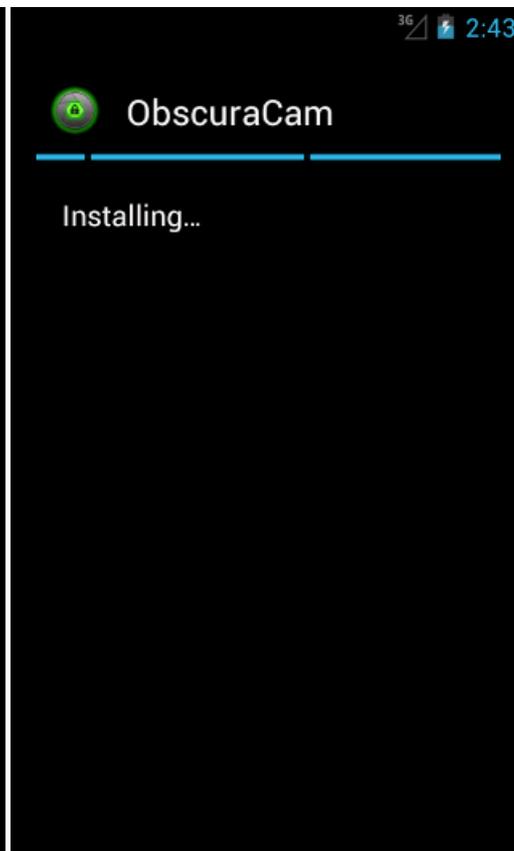
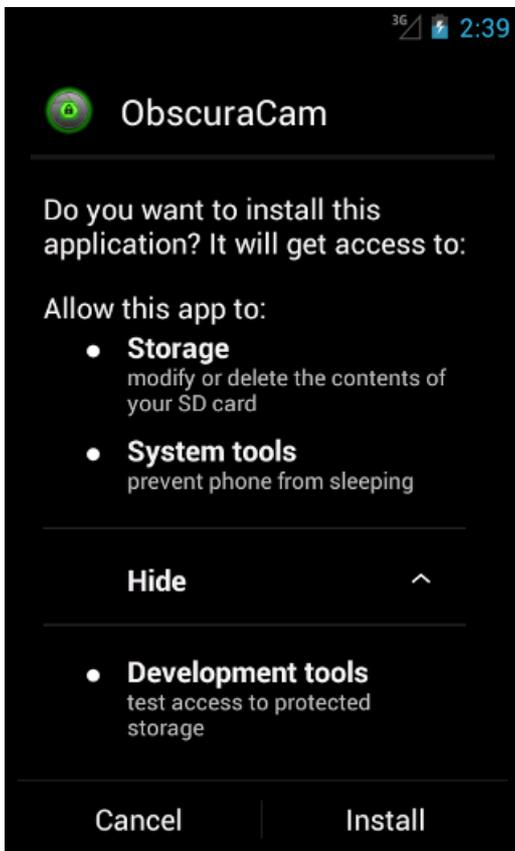
2.0 Comment installer *ObscuraCam*

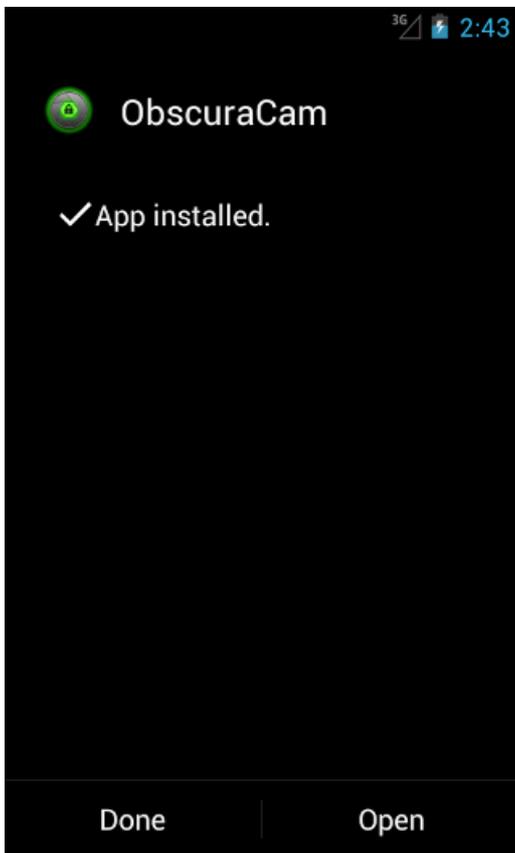
Étape 1. Téléchargez l'application à partir de la boutique [Google Play](#) [40]



Graphique 1 : ObscuraCam dans la boutique Google Play

Étape 2. Confirmez les autorisations demandées par l'application et démarrez l'installation en appuyant sur la touche **Install**.

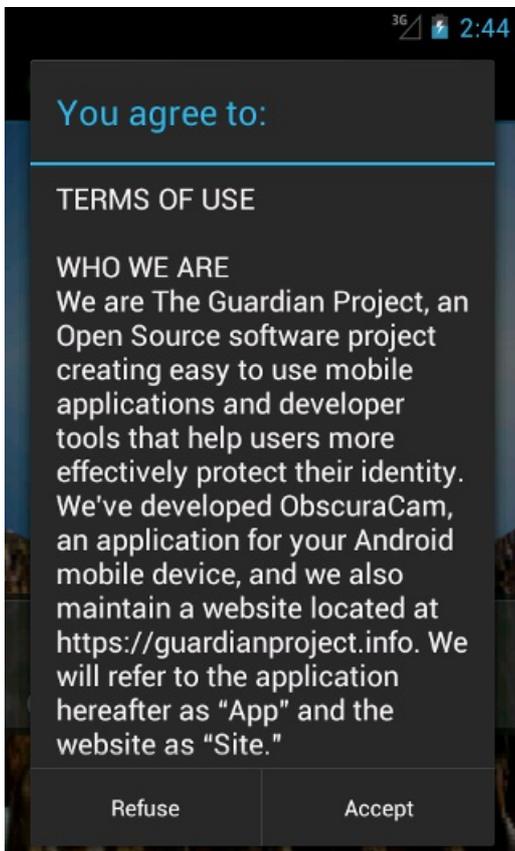




Graphiques 3, 4 et 5 : Confirmation des autorisations et de la procédure d'installation

Étape 3. Appuyez sur *Open* (ouvrir) pour démarrer l'application une première fois.

**** Étape 4.**** Lisez les *conditions d'utilisation* attentivement. Vous pouvez **accepter** en appuyant sur *Accept*.



Graphique 6 : Conditions d'utilisation

2.1 Prendre des photos avec ObscuraCam

Vous pouvez utiliser **ObscuraCam** pour masquer certains ou tous les visages qui apparaissent sur vos photos. Ceci

fonctionne sur les photos que vous avez prises avec l'application **ObscuraCam**, mais vous pouvez également brouiller les visages sur d'autres photos s'il vous est possible de copier ou de déplacer les fichiers photo sur votre appareil Android.

Pour prendre une photo avec votre appareil Android sans montrer les visages des personnes, suivez les étapes suivantes :

Étape 1. Appuyez sur la touche **Camera** (appareil-photo)



Graphique 7 : Écran d'accueil d'ObscuraCam

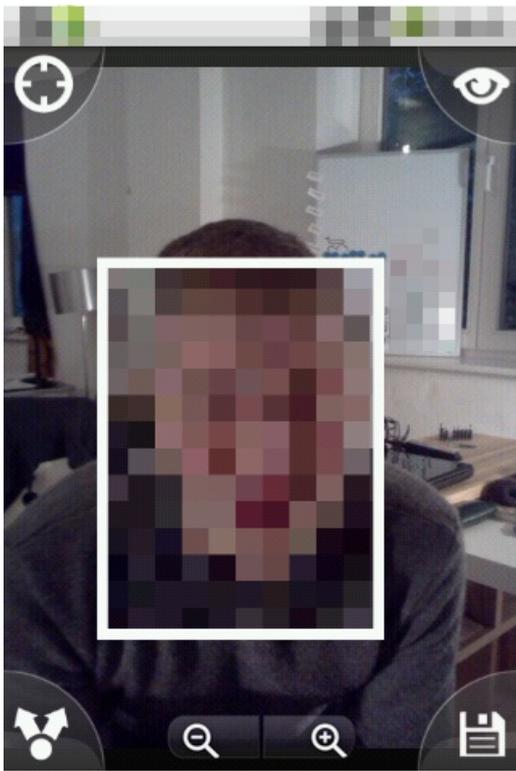
Étape 2. Prenez une photo en cliquant sur



Étape 3. Appuyez sur la touche de sauvegarde **Save** en cliquant sur



ObscuraCam tentera d'identifier les visages automatiquement. Pour chaque visage qu'elle reconnaît, elle va ajouter un "tag" (un rectangle utilisé pour sélectionner le contenu à cacher).

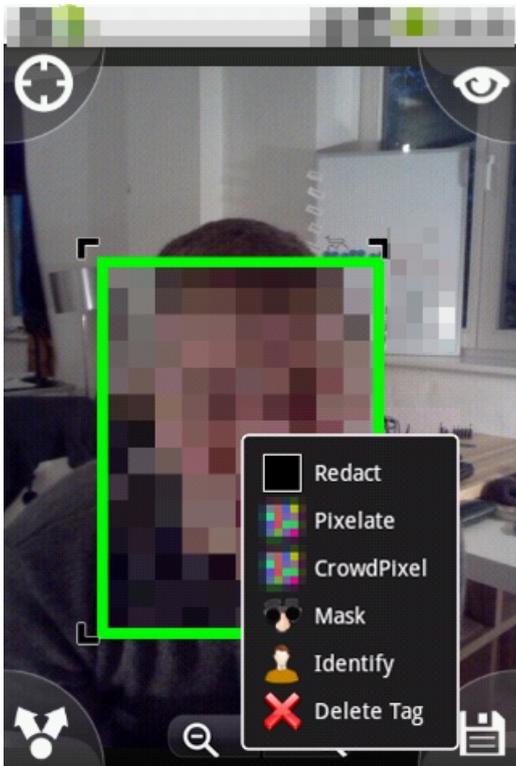


Graphique 8 : Un visage « taggé » automatiquement

Étape 4. Sélectionnez ou modifiez le contenu que vous souhaitez cacher

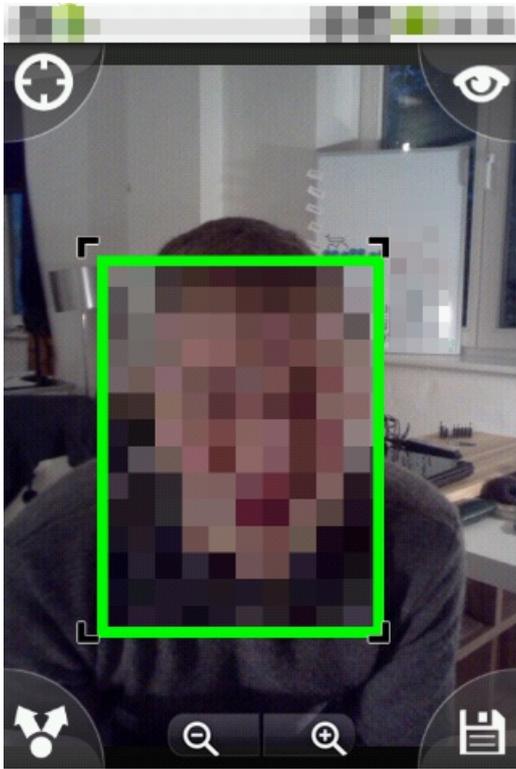
Les tags de photos peuvent être modifiés des façons suivantes :

- **Appuyez** sur une partie de votre photo que vous souhaitez cacher pour y ajouter un tag.
- **Appuyez** sur un tag existant (le contour devrait s'allumer en vert), puis appuyez sur *Delete Tag* pour le supprimer



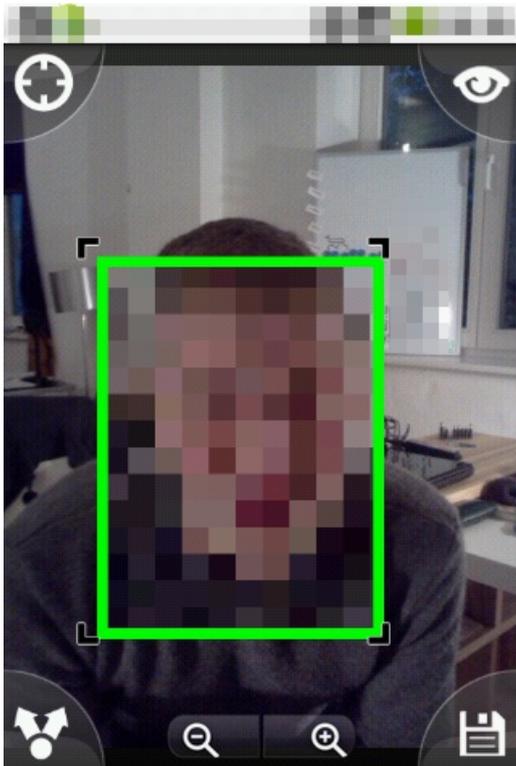
Graphique 9 : Options de taggage

Appuyez et faites **glisser** le centre d'un tag pour le déplacer (ce qui changera la partie de la photo à cacher).



Graphique 10 : Déplacement d'un tag

Appuyez et faites **glisser** au plus près d'un des côtés du tag (mais à l'intérieur du rectangle) pour modifier la taille et la forme du tag.

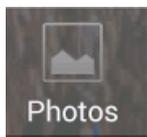


Graphique 11 : Redimensionner un tag

2.2 Masquer les visages dans des photos déjà existantes

Pour cacher les visages dans une photo déjà existante, suivez les étapes suivantes :

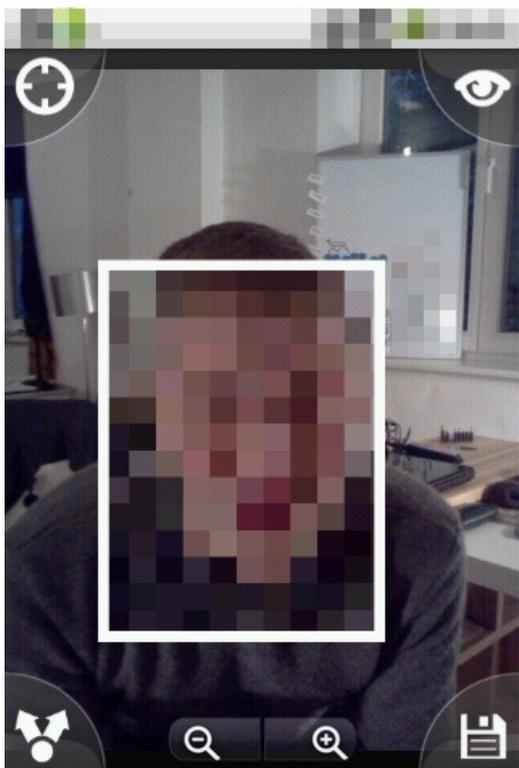
Étape 1. Copiez ou déplacez le fichier photo souhaité sur votre appareil Android s'il n'y est pas déjà.



Étape 2. Appuyez sur la touche

Étape 3. Sélectionnez la photo que vous souhaitez modifier.

ObscuraCam tentera d'identifier les visages **automatiquement**.

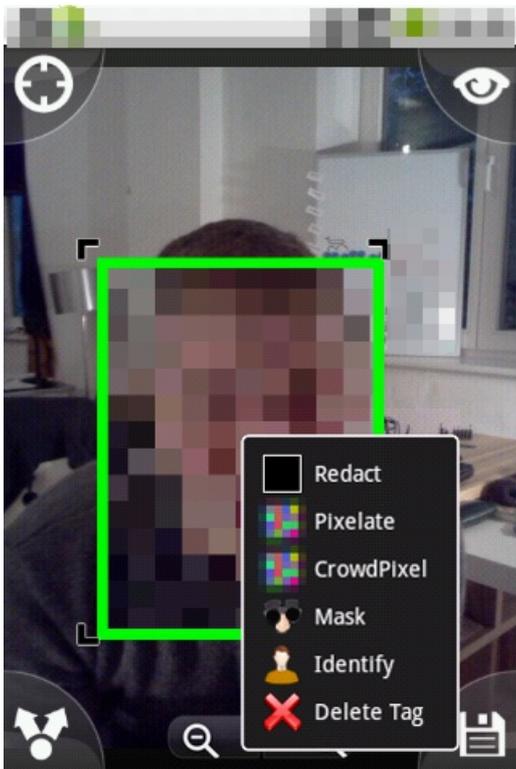


Graphique 12 : Visage détecté automatiquement

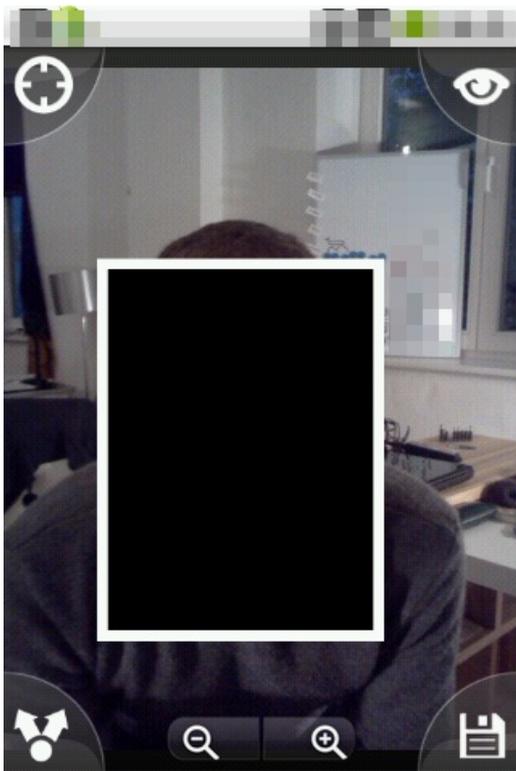
Étape 4. Sélectionnez ou modifiez le contenu que vous souhaitez cacher.

2.3 Modifier le mode « flou »

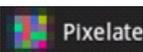
Il existe plusieurs moyens et façons différents de brouiller un visage dans une photo. Cliquez sur le centre du contour vert de la photo pour voir les différentes options indiquées ci-dessous

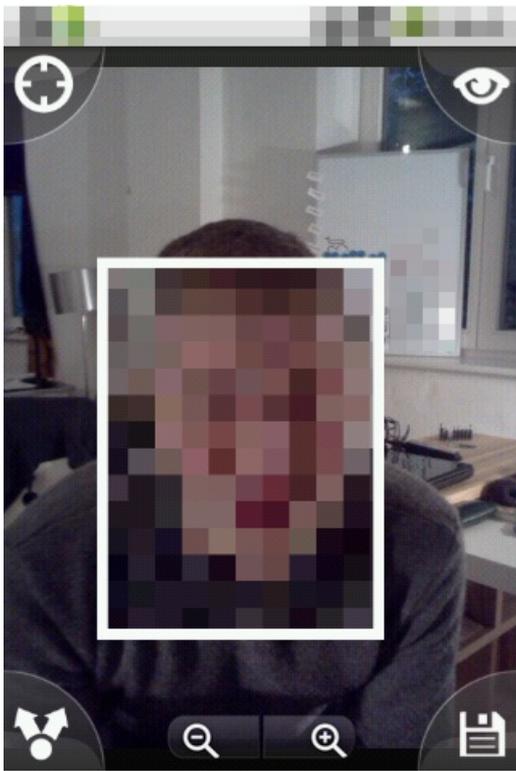


Première option : Si vous cliquez sur , votre photo ressemblera à ce qui suit :

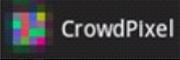


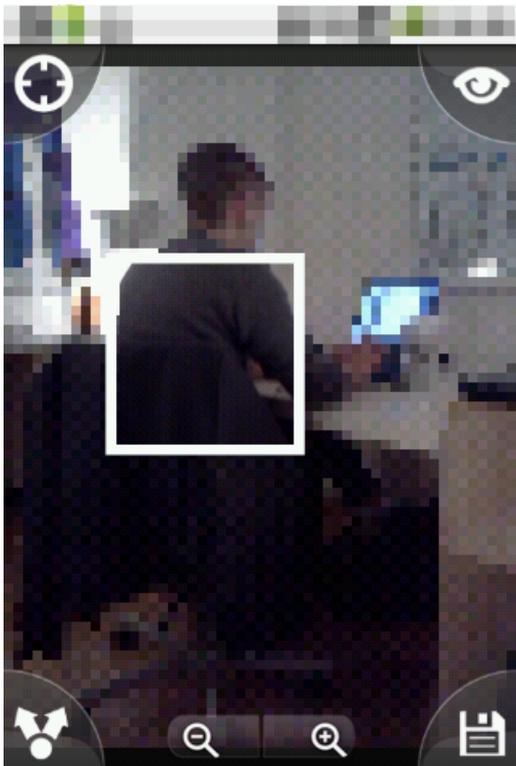
Graphique 13 : Un visage supprimé

Seconde option : Si vous cliquez sur , votre photo ressemblera à ce qui suit :



Graphique 14 : Un visage pixelisé

Troisième option : Si vous cliquez sur , l'espace **en dehors** de la sélection va être pixelisé et votre photo ressemblera à ce qui suit :



Graphique 15 : Une photo pixelisée en large

Quatrième option : Si vous cliquez sur , votre photo ressemblera à ce qui suit :



Graphique 16 : Un visage masqué

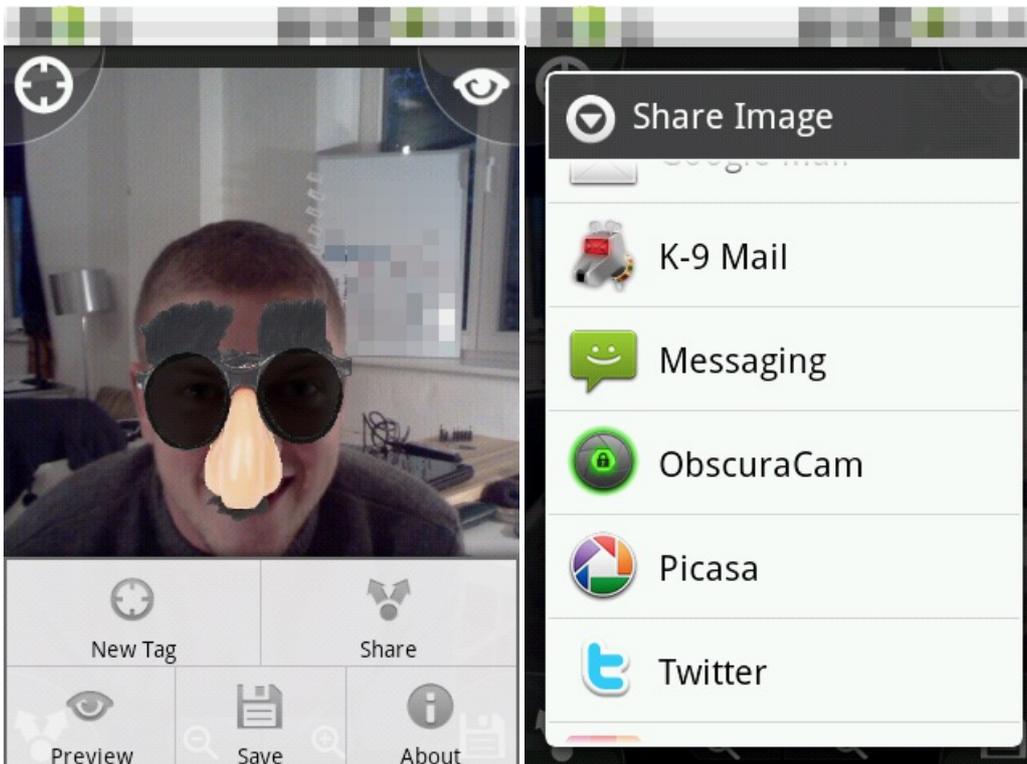
2.4 Partager des photos

Note : Assurez-vous que vous supprimez toutes les métadonnées des photos que vous prenez avec votre téléphone Android avant de partager celles-ci avec qui que ce soit. Le fait de cacher l'identité d'une personne photographiée avec **Obscuracam** ne supprime pas les métadonnées qui comprennent de nombreux détails tels que la localisation, les spécifications de l'appareil-photo et d'autres informations.

Vous pouvez partager les photos que vous avez créées avec **Obscuracam** en suivant les étapes suivantes :



Étape 1. Cliquez sur  ou sur *Menu* puis sur *Share* (partager) pour ouvrir les options de partage d'images.



Graphiques 17 et 18 : Options de partage d'images

Étape 2. Choisissez le service que vous souhaitez utiliser pour partager l'image de votre choix avec votre réseau.

2.5 Supprimer les fichiers multimédia d'origine

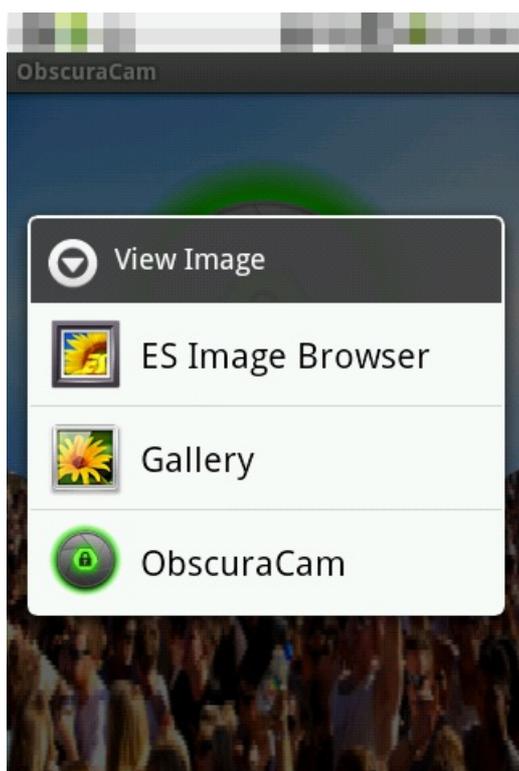
Étape 1. En cliquant sur Save (sauvegarder), une fenêtre va apparaître, vous demandant si vous souhaitez supprimer le fichier multimédia d'origine.



Graphique 18 : Option de suppression

Étape 2. Cliquez sur **Yes** (oui) si le fichier médiatique original se trouvant sur votre smartphone constitue un risque pour vous-même ou d'autres personnes.

Étape 3. Si vous souhaitez supprimer une photo d'une galerie ou d'un album photo, **sélectionnez** tout d'abord la photo que vous souhaitez supprimer de votre galerie ou toute autre application d'aperçu des images que vous utilisez.



Graphique 19 : Menu

Étape 4. Cliquez sur **Delete** (supprimer) comme indiqué ci-dessous



Graphique 20 : Option de suppression

Note : Avec Android 2.2, il se peut que vous ne puissiez pas supprimer les fichiers multimédia d'origine. Dans ce cas, connectez votre appareil Android avec votre ordinateur de façon à pouvoir supprimer l'image originale.

Orbot pour appareils Android

Short Description:

Orbot est une application de téléphonie mobile de la plateforme Android, créée par le [Guardian Project](#) [16] pour améliorer l'anonymité de vos activités sur Internet.

Online Installation Instructions:

Télécharger Orbot

À partir du site web officiel

- Lisez l'introduction courte des [guides pratiques](#) [3]
- Cliquez sur l'icône **Orbot** ci-dessous pour ouvrir <https://guardianproject.info/apps/>
- Défilez vers le bas jusqu'à ce que vous voyiez l'icône d'**Orbot**, cliquez ensuite sur **Download App** (télécharger l'application)
- Cliquez sur la touche **Install** (installer) dans Google Play
- Une fois installée, cliquez sur **open** (ouvrir) pour démarrer l'application

À partir de Google Play

- Vous pouvez également installer **Orbot** à partir de [Google Play](#) [41]
- Une fois installée, cliquez sur **Open** (ouvrir) pour démarrer l'application

Orbot:



[22]

Page d'accueil

- [Page d'accueil d'Orbot](#) [42]
- [Site du développeur d'Orbot](#) [42]

Téléphone requis

- Android 1.6 et plus récent

Version utilisée dans ce guide

- Orbot : 1.0.9-RC4-tor-0.2.3.17-beta

Licence

- Freeware - BSD

Lecture requise

- Livret pratique, chapitre **8. Préserver votre anonymat et contourner la censure sur Internet** ^[14]
- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** ^[9]
- Livret pratique, chapitre **11. Utiliser votre smartphone en sécurité (autant que possible...)** ^[10]

Niveau : 1 : Débutant, 2 : Moyen, 3 : *Intermédiaire*, 4 : Expérimenté, 5 : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 10 minutes

Ce que vous obtenez en retour :

- La faculté de cacher votre identité numérique lorsque vous visitez des sites Internet ou lors d'autres activités impliquant l'utilisation de certaines autres applications Android. -La faculté de cacher vos activités de navigation et de chats aux fournisseurs d'accès Internet (FAI) et autres mécanismes de surveillance intervenant lors de l'utilisation de certaines autres applications Android.
- La faculté de contourner la censure sur Internet et les règles de filtrage lorsque vous naviguez avec certaines autres applications Android.

1.1 Ce que vous devez savoir sur cet outil avant de commencer

Orbot fournit aux appareils Android l'accès au réseau Tor ^[43]. Pour plus d'informations, consultez **Tor - anonymat et contournement sur Internet** ^[44].

2 Comment installer et utiliser Orbot

Liste des sections:

- **2.0 Comment installer Orbot**
 - **2.1 Comment utiliser Orbot**
 - **2.2 Naviguer sur Internet dans l'anonymat**
-

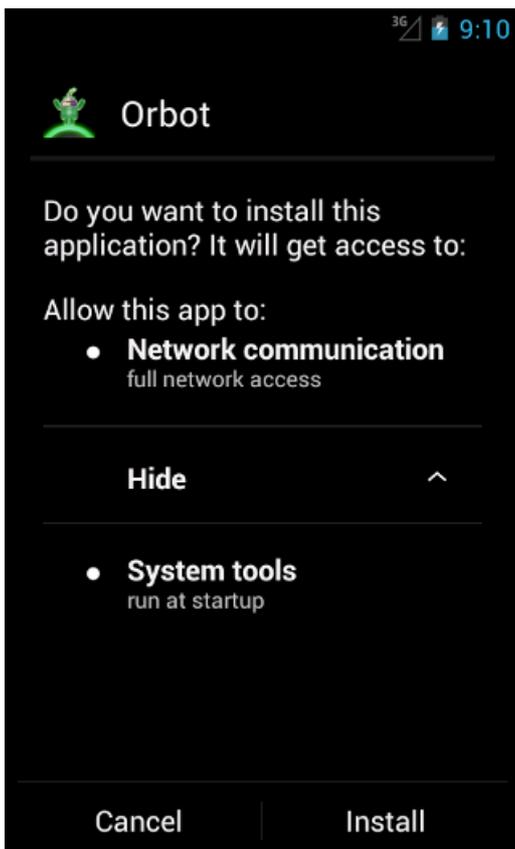
2.0 Comment installer Orbot

Étape 1. Téléchargez l'application à partir de la boutique Google Play ^[41].



Graphique 1 : Orbot dans la boutique Google Play

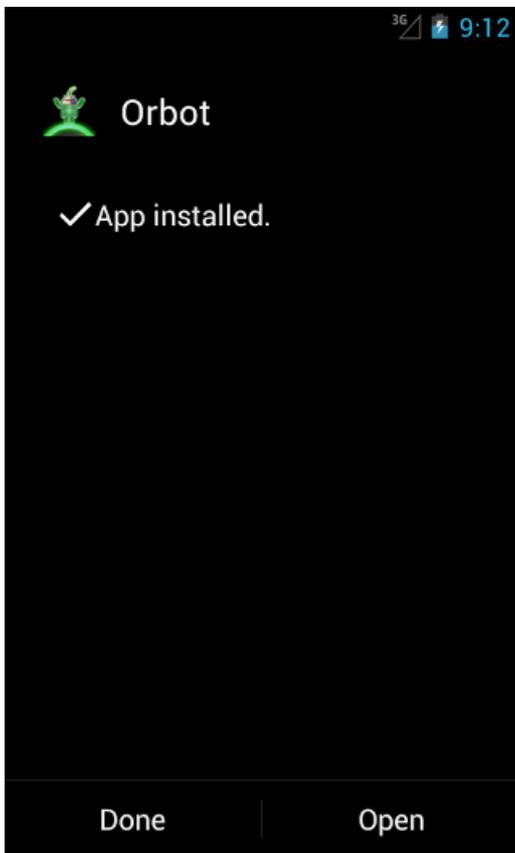
Étape 2. Lisez et confirmez les autorisations requises par l'application et installez l'application en appuyant sur la touche *Install*.



Graphique 2 : Autorisations requises

2.2 Utiliser Orbot pour la première fois

Étape 1. Appuyez sur *Open* (ouvrir) pour démarrer **Orbot** une première fois.



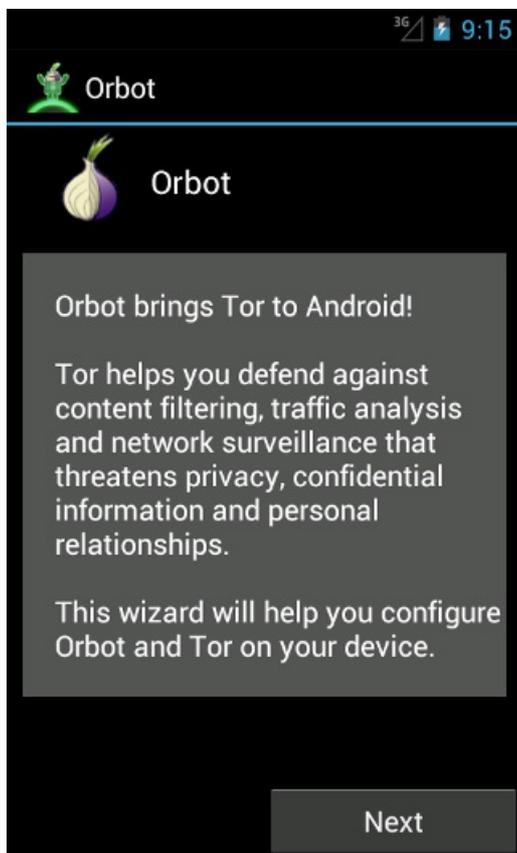
Graphique 3 : Application installée

Étape 2. Choisissez la langue que vous souhaitez et appuyez sur *Next* (suivant).



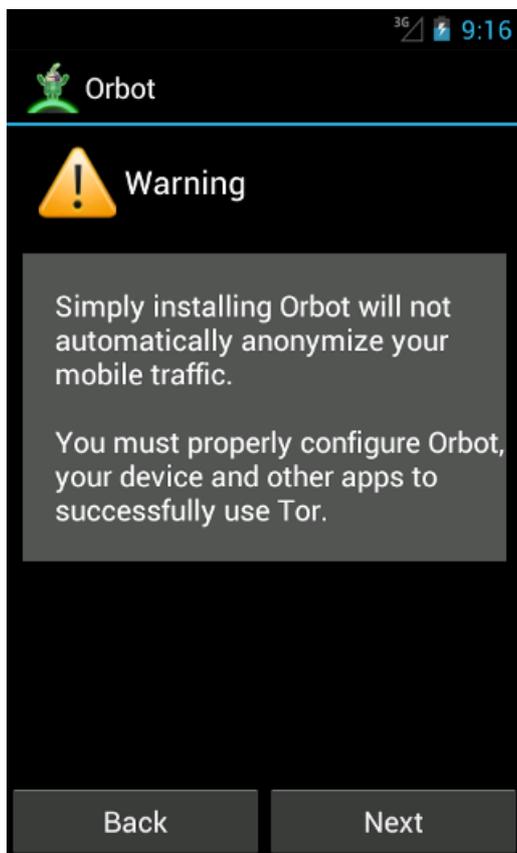
Graphique 4 : Choisir la langue

Étape 3. Un assistant de configuration apparaîtra muni d'une description du projet Tor et d'Orbot. **Lisez-la**, puis appuyez sur *Next* (suivant).



Graphique 5 : Informations sur Orbot

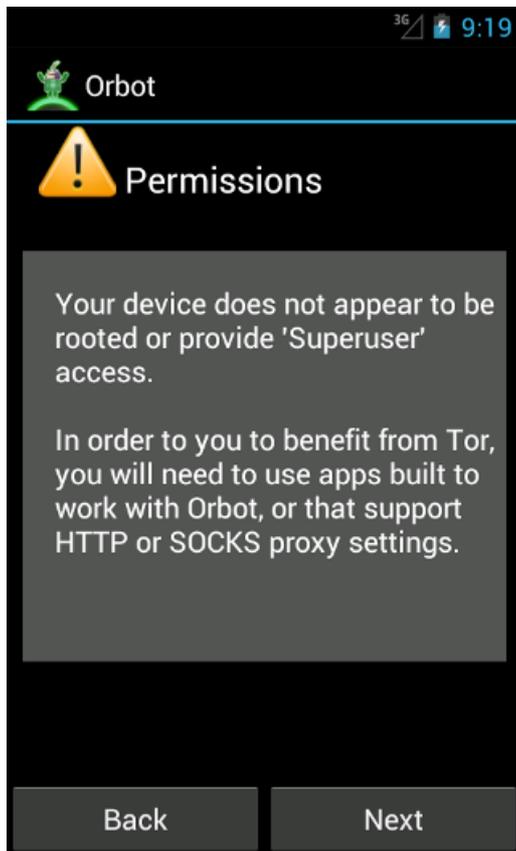
Step 4. Un avertissement apparaîtra dans l'écran. **Lisez-le**, puis appuyez sur *Next*.



Graphique 6 : Avertissement important quant à la façon d'utiliser Orbot

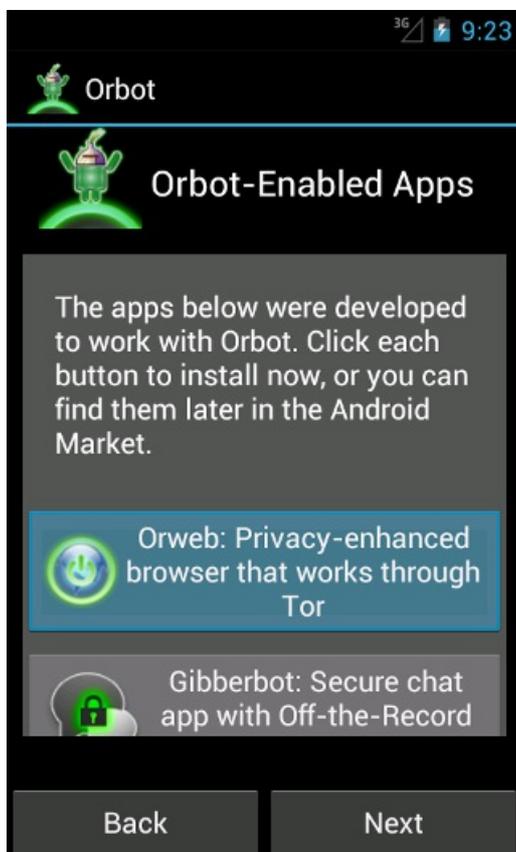
Étape 5. Un écran d'autorisation peut parfois apparaître, vous informant si votre appareil n'est pas rooté ^[43] (ou débridé) et vous demandant si vous souhaitez les fonctionnalités « Superuser » (super-utilisateur) d'Orbot Transparent Proxy (consultez Sécurité avancée pour votre smartphone ^[45]). Dans ce guide, nous n'examinons pas cette option. Si votre smartphone n'est pas rooté, il vous suffit de **cocher** l'option indiquant *I understand and would like to continue without Superuser* (Je comprends et je voudrais continuer sans Superuser). Pour bénéficier de Tor, il vous faudra utiliser des

applications conçues pour fonctionner avec **Orbot** ou compatibles avec http ou socks.



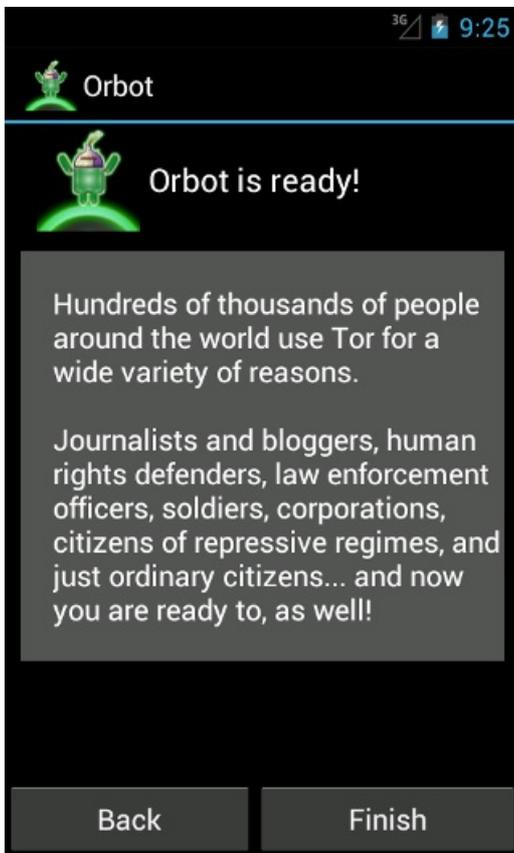
Graphique 7 : Note concernant le rooting

Étape 6. Une liste d'applications fonctionnant avec **Orbot** va apparaître. Prenez-les en considération, puis appuyez sur *Next* (suivant).



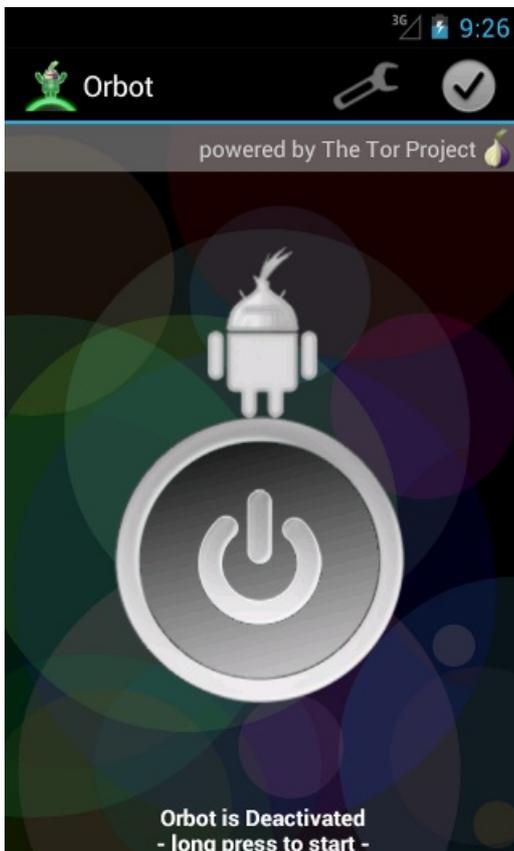
Graphique 8 : Applications compatibles avec Orbot

Étape 7. Continuez la lecture, puis appuyez sur *finish* (terminer).



Graphique 9 : Orbot est prête !

Étape 8. Une grande icône grise **Orbot** apparaîtra. L'application est maintenant installée et configurée.



Graphique 10 : Orbot désactivée

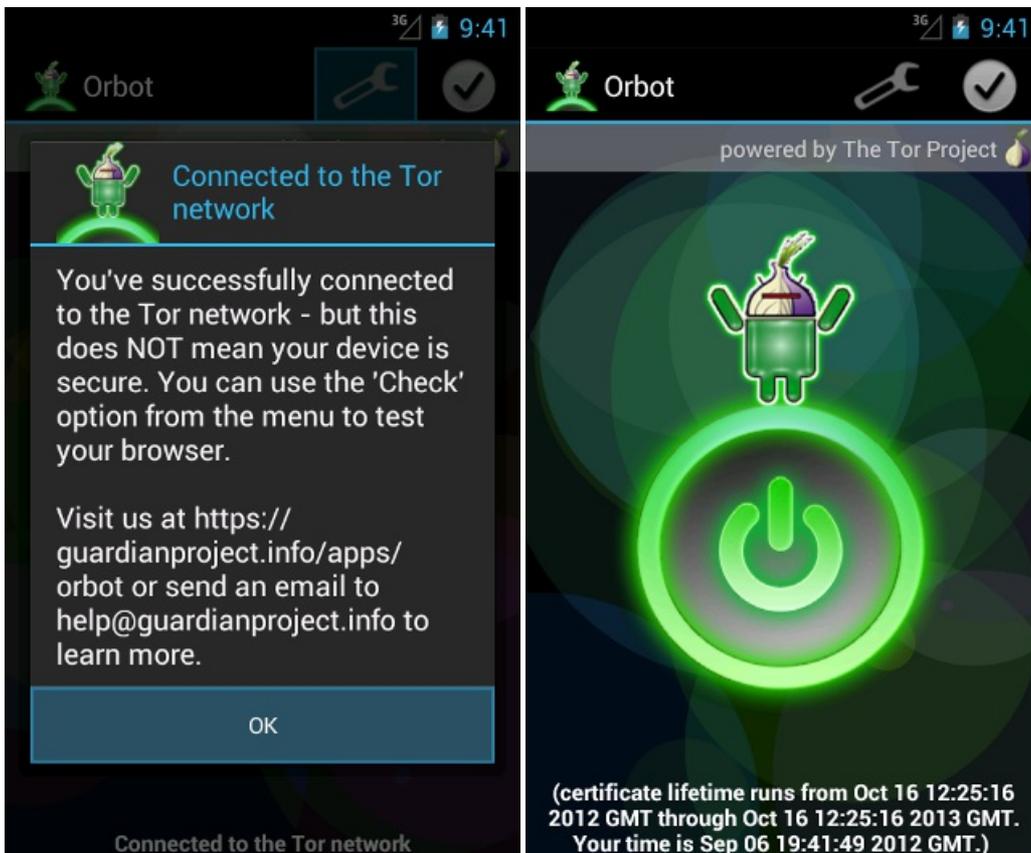
2.1 Comment utiliser Orbot

Étape 1. Appuyez en maintenant la pression sur l'icône **Orbot** pour allumer ou éteindre **Orbot**. Elle passe ainsi du gris au jaune, comme ci-dessous.



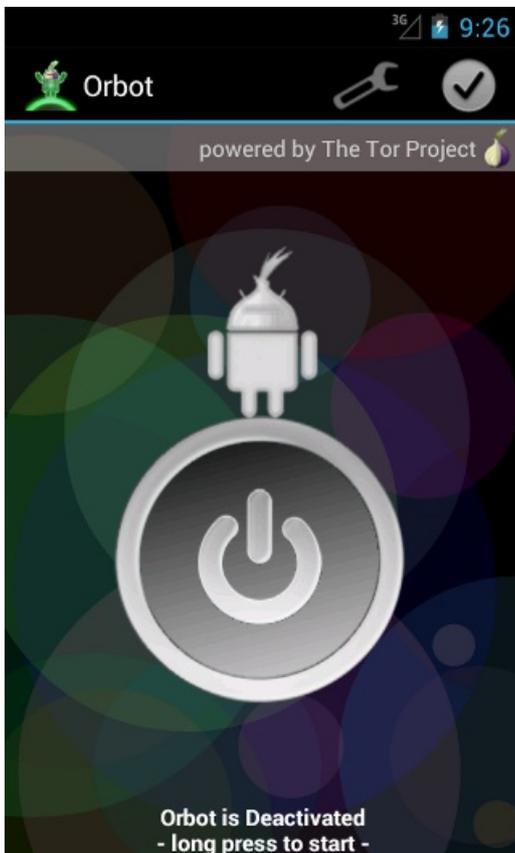
Graphiques 11 et 12 : Activer Orbot

Étape 2. Un texte apparaîtra pour vous informer que vous êtes bien connecté au réseau Tor. Cliquez sur OK.



Graphiques 12 et 13 : Orbot parachève la connexion

Étape 3. ****Appuyez en maintenant la pression** sur l'icône verte jusqu'à ce que celle-ci passe au gris pour éteindre Orbot.



2.2 Naviguer sur Internet dans l'anonymat

Pour naviguer sur Internet de façon anonyme, il vous faut installer une application de navigateur qui puisse faire passer votre communication par un serveur mandataire (ou Proxy) en conjonction avec **Orbot**, ainsi qu'une application de messagerie instantanée accomplissant la même chose. Merci de consulter les *guides pratiques* connexes à l'utilisation d'**Orweb** [46] et de **Gibberbot** [47] avec **Orbot**.

Orweb pour appareils Android

Short Description:

Orweb est une application libre de téléphonie mobile de la plateforme Android, créée par le Guardian Project [16] pour une navigation anonyme sur le web en conjonction avec **Orbot** [48].

Online Installation Instructions:

Télécharger Orweb

À partir du site web officiel

- Lisez l'introduction courte des *guides pratiques* [3]
- Cliquez sur l'icône **Orweb** ci-dessous pour ouvrir <https://guardianproject.info/apps/>
- Défilez vers le bas jusqu'à l'icône **Orweb** puis cliquez sur **Download app** (télécharger l'application)
- Cliquez la touche **Install** (installer) dans Google Play
- Une fois installée, cliquez **Open** (ouvrir) pour démarrer l'application

À partir de Google Play (Android FOSS repository)

- Vous pouvez également installer **Orweb** à partir de **Google Play** [49]
- Une fois installée, cliquez **Open** (ouvrir) pour démarrer l'application

Orweb:



[22]

Page d'accueil

Page d'accueil d'Orweb [50]

Matériel requis

- Android 1.6 ou plus récent

Version utilisée dans ce guide

- v2 (0.2.2)

Licence

- FOSS (GPLv3)

Lecture requise

- Livret pratique, chapitre **8. Préserver votre anonymat et contourner la censure sur Internet** ^[14]
- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** ^[9]
- Livret pratique, chapitre **11. Utiliser votre smartphone en sécurité (autant que possible...)** ^[10]

Niveau 1 : Débutant, 2 : Moyen, 3 : Intermédiaire, 4 : Expérimenté, 5 : Avancé

Temps nécessaire pour commencer à utiliser cet outil : 20 minutes

Ce que vous obtenez en retour :

- La faculté de cacher votre identité numérique aux sites que vous visitez.
- La faculté de cacher vos destinations en ligne aux fournisseurs d'accès à Internet (FAIs) et autres mécanismes de surveillance.
- La faculté de contourner la censure et les règles de filtrage.

Applications compatibles avec Android, iPhone, Blackberry :

1.1 Ce que vous devez savoir sur cet outil avant de commencer

Orweb ne fonctionnera correctement qu'après l'installation et la configuration d'**Orbot** ^[48]. Rappelez-vous que si vous accédez à une messagerie ou à un blog créés précédemment avec **Orweb**, le site ne pourra certes pas définir votre localisation actuelle mais il vous reconnaîtra. Si vous souhaitez que les choses se fassent dans l'anonymat complet, il vous faudra ne jamais accéder à vos utilisateurs « réels », ni ne transmettre de données personnelles ou faire les mêmes choses que lorsque vous ne cherchez pas à rester anonyme.

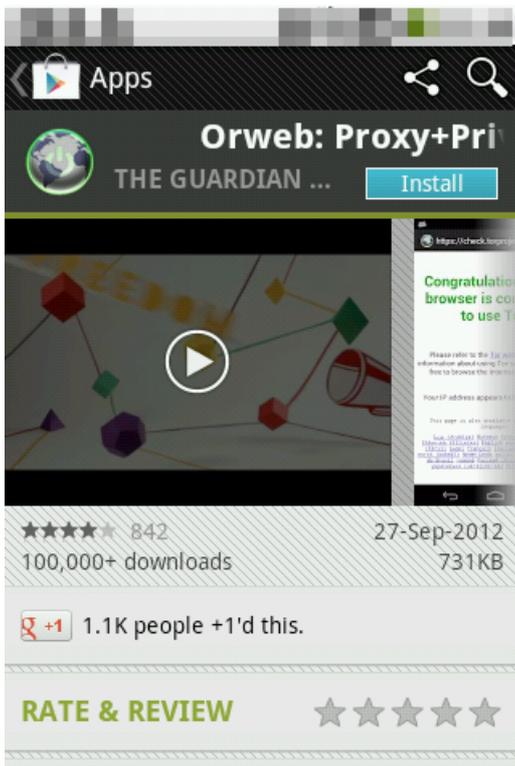
2. Comment installer et utiliser Orweb

Liste des sections :

- **2.0 Comment installer Orweb**
 - **2.1 Comment naviguer avec Orweb**
 - **2.2. Alternatives avancées**
-

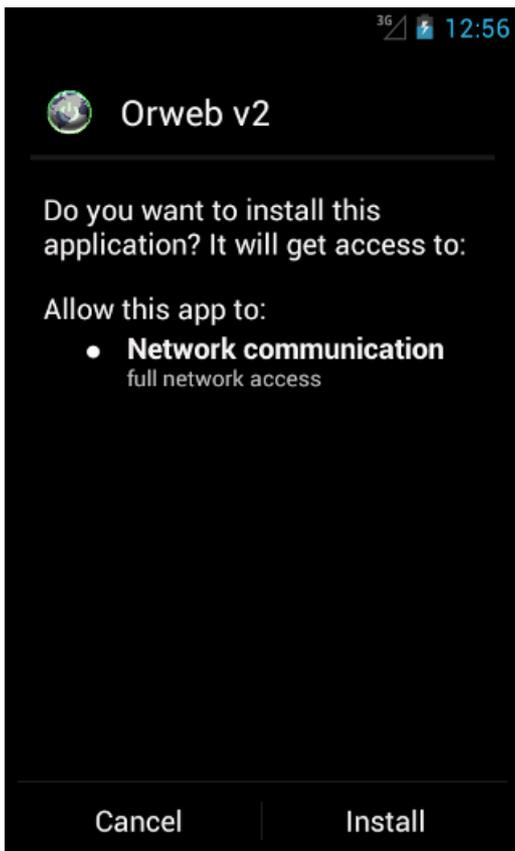
2.0 Comment installer Orweb

Étape 1. Téléchargez l'application à partir de la boutique [Google Play](#) ^[51].



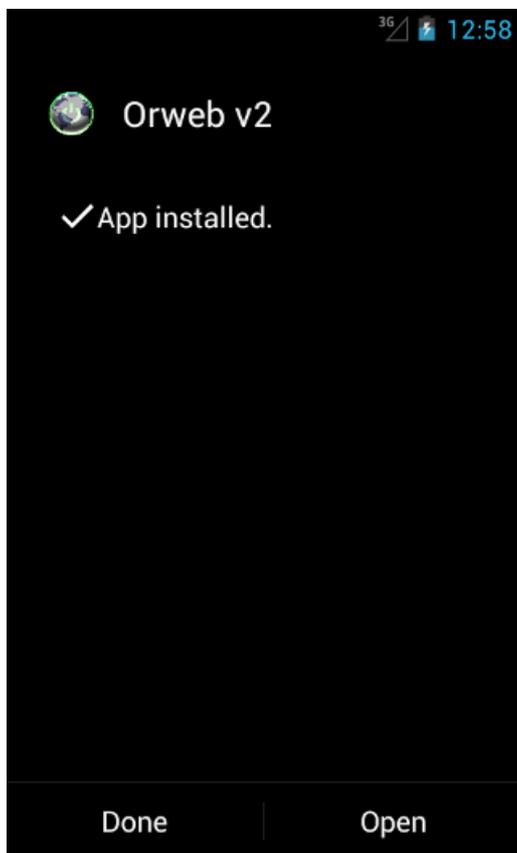
Graphique 1 : Orweb dans la boutique Google Play

Étape 2. Confirmez les autorisations requises par l'application et installez-la en appuyant sur la touche **Install**.



Graphiques 2 : Autorisations

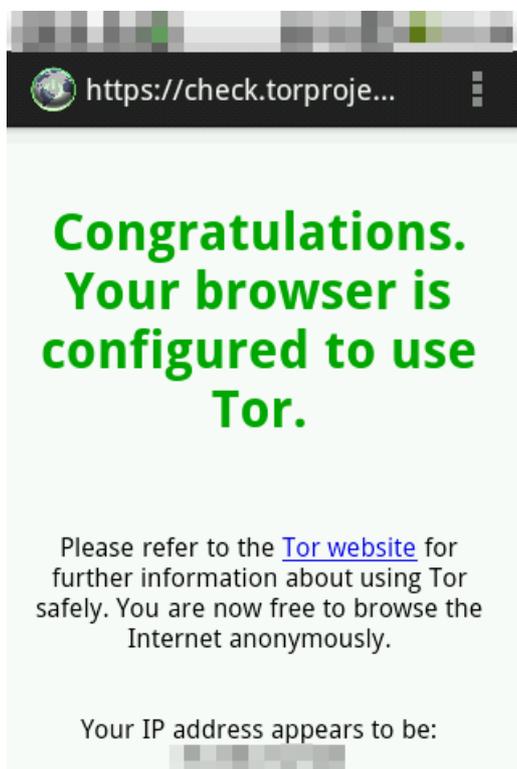
Étape 3. Une fois l'application installée, vous devriez voir cet écran.



Graphique 3 : Confirmation de l'installation

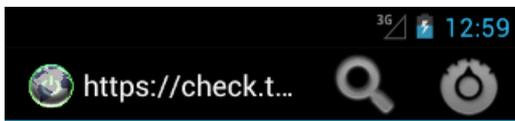
2.1 Comment naviguer avec Orweb

Étape 4. Une fois l'installation terminée, **appuyez** sur « Open » (ouvrir) pour démarrer l'application une première fois. Si vous avez activé **Orbot** avant d'accéder à **Orweb**, un écran apparaîtra pour vérifier que votre anonymat dans le navigateur web est assuré.



Graphique 4 : Confirmation de votre connexion au réseau Tor.

Si **Orbot** n'est pas activé ou ne fonctionne pas correctement, un écran d'erreur apparaîtra dans **Orweb**.



Webpage not available

The webpage at <https://check.torproject.org/> might be temporarily down or it may have moved permanently to a new web address.

Suggestions:

- Make sure you have a data connection
- Reload this webpage later
- Check the address you entered

Graphique 5 : Écran d'erreur

2.2 Alternatives avancées

Si vous avez besoin d'un meilleur navigateur qu'**Orweb** garantissant l'anonymat, nous vous recommandons d'installer **Firefox Mobile** et d'en configurer le proxy de façon à utiliser **Orbot**, quoique vous risquez de perdre certaines fonctionnalités de sécurité.

TextSecure pour appareils Android

Short Description:

TextSecure est une application de téléphonie mobile de la plateforme Android, conçue pour chiffrer les messages textuels (SMS) lors de leur envoi ou de leur conservation sur votre téléphone.

Online Installation Instructions:

Télécharger TextSecure

À partir du site web officiel

- Lisez l'introduction courte des **guides pratiques** ^[3]
- Cliquez sur l'icône **TextSecure** ci-dessous pour ouvrir <http://www.whispersys.com/>
- Vous pouvez scanner le code QR placé à côté de l'icône **TextSecure** pour aller à l'application. Cliquez sur la touche **Install** (installer) dans Google Play
- Une fois installée, cliquez sur **open** (ouvrir) pour démarrer l'application

À partir de Google Play

- Vous pouvez également installer **TextSecure** à partir de **Google Play** ^[52]
- Une fois installée, cliquez sur **open** (ouvrir) pour démarrer l'application

TextSecure:



^[53]

Page d'accueil

- www.whispersys.com ^[54]

Téléphone requis

- Android 1.6 et plus récent

Version utilisée dans ce guide

- 0.5.7

Licence

- Freeware GPL-V3

Lecture requise

- Livret pratique, chapitre **9. Utiliser votre téléphone mobile en sécurité (autant que possible...)** ^[9]

Temps nécessaire pour commencer à utiliser cet outil : 10 minutes

Ce que vous obtenez en retour :

- La faculté de chiffrer vos messages SMS lors de leur envoi à d'autres utilisateurs de TextSecure.
- Vos messages sont stockés sur votre appareil dans une base de données chiffrée, protégée par une phrase secrète.
- Si vous perdez votre téléphone ou qu'il vous est volé, vos messages seront illisibles pour ceux qui ne connaissent pas votre phrase secrète.

1.1 Ce que vous devez savoir sur cet outil avant de commencer

- Grâce à cette application, personne ne pourra lire le contenu de vos SMS. Par contre, ceci ne cachera pas le fait que vous envoyez des messages, ni la destination de ceux-ci.
 - Pour établir une connexion sécurisée, **TextSecure** va nécessiter un échange de SMS : les deux parties concernées vont envoyer ET recevoir un message leur demandant d'établir la connexion. Cette opération n'est donc pas gratuite.
 - Dans certains pays, un programme de chiffrement tel que **TextSecure** peut être illégal ou soumis à des contraintes juridiques.
-

2. Comment installer et utiliser TextSecure

Liste des sections :

- **2.0 Comment installer TextSecure**
 - **2.1 Configuration et première installation**
 - **2.2 Établir une communication sécurisée**
 - **2.3 Vérification de l'identité**
 - **2.4 Échanger des messages chiffrés**
-

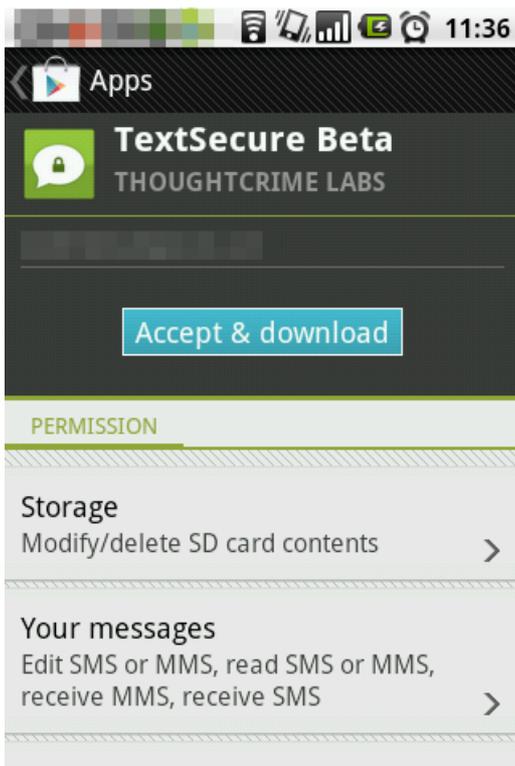
2.0 Comment installer *TextSecure*

Étape 1. Téléchargez l'application à partir de la boutique [Google Play](#) ^[55]



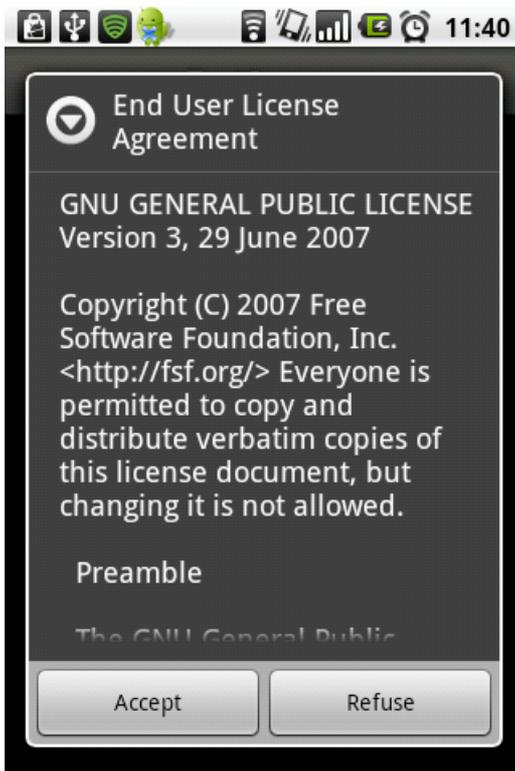
Graphique 1 : TextSecure dans la boutique Google Play.

Étape 2. Installez l'application (en **cliquant** la touche d'installation appropriée).



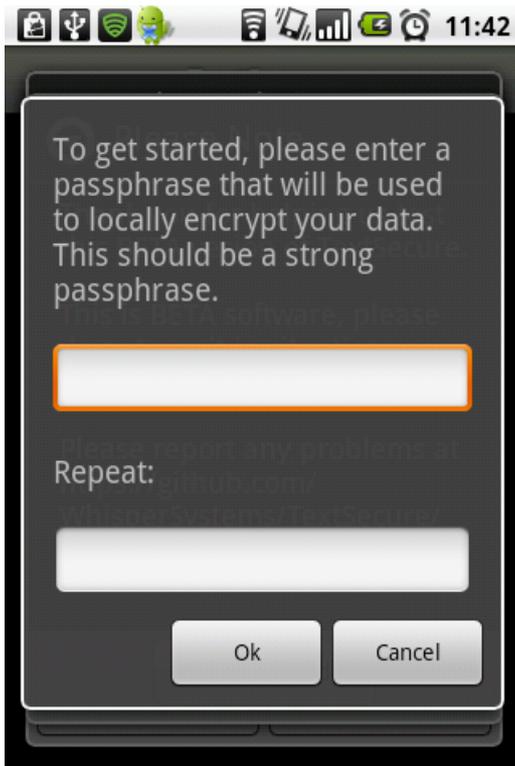
Graphique 2 : Autorisations nécessaires pour télécharger.

Étape 3. Lisez et acceptez la licence GNU [43].



Graphique 3 : Contrat de licence utilisateur final.

Étape 4. Créez un mot de passe ou une phrase secrète pour chiffrer les données stockées sur votre téléphone



Graphique 4 : Créez et répétez le mot de passe ou phrase secrète

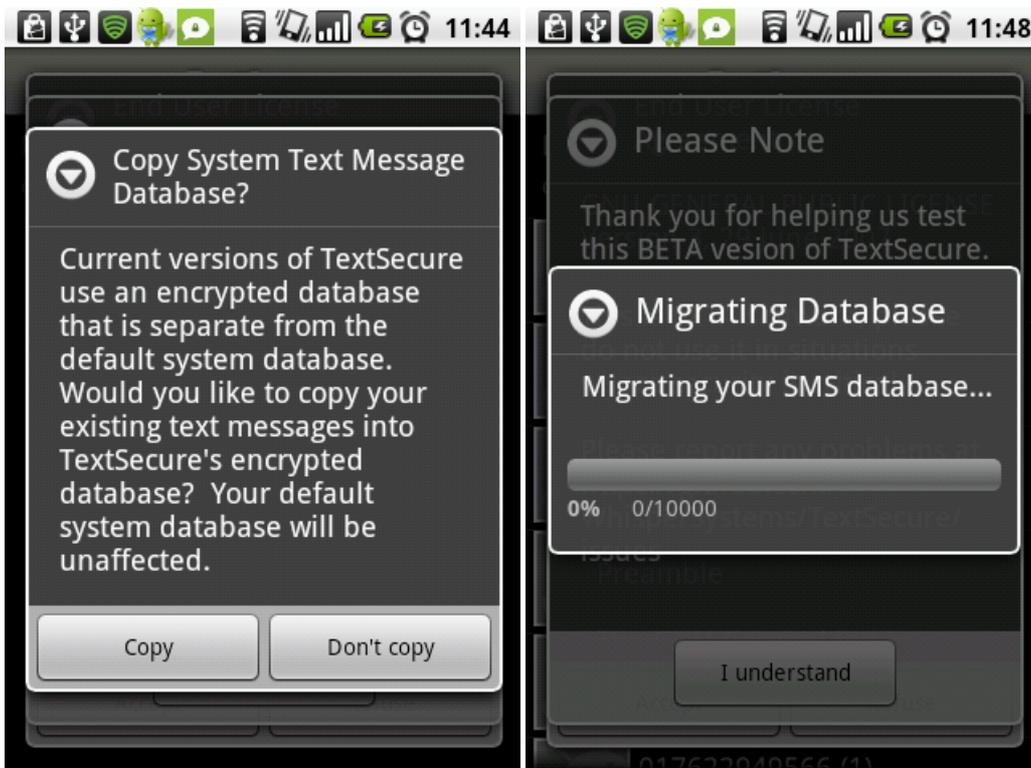
2.1 Configuration et première installation

Étape 1. Cliquez sur l'icône TextSecure et entrez votre mot de passe TextSecure.



Graphique 5 : Entrer le mot de passe ou phrase secrète

Étape 2. L'application va vous demander si vous souhaitez copier la base de données de messages textuels sur votre téléphone. Il est recommandé de **copier** vos messages afin qu'ils soient chiffrés, puis de les **effacer** de leur ancien emplacement.



Graphiques 6 et 7 : Migration de la base de données SMS

Étape 3. Assurez-vous que vos anciens messages apparaissent dans la boîte de réception de l'application **TextSecure**.

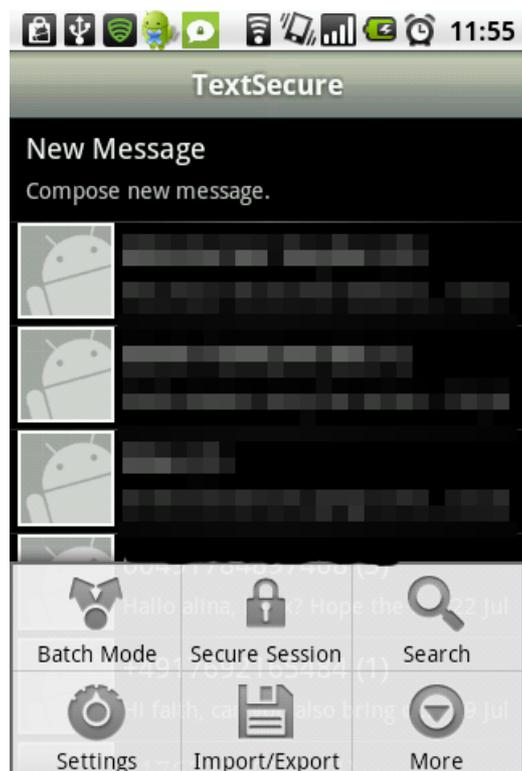
Étape 4. Effacez vos messages de leur ancien emplacement.

À ce stade, vous êtes prêt à utiliser *TextSecure*** comme application de messagerie SMS. **Note :** Si vous ne souhaitez pas échanger de messages chiffrés, vous pouvez toujours utiliser **TextSecure** pour *stocker en toute sécurité les messages que vous envoyez et recevez ; ce qui signifie que si vous perdez votre téléphone, vos messages seront indéchiffrables par toute personne devant le trouver.

2.2 Établir une communication sécurisée

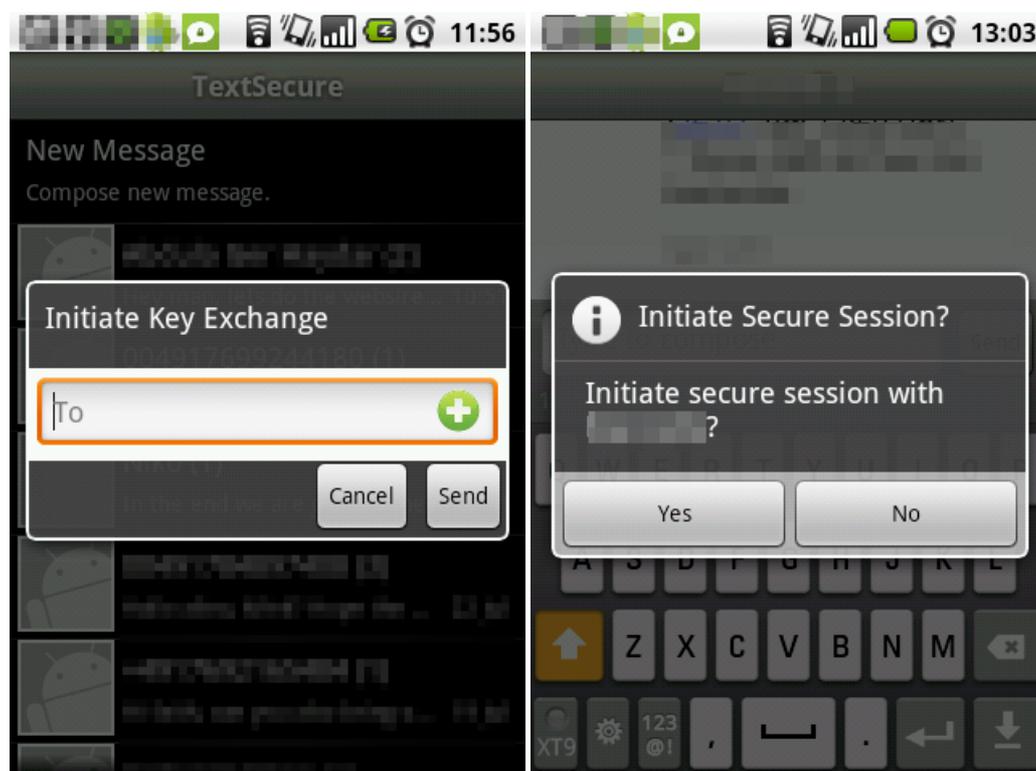
Il est nécessaire d'effectuer une première sécurisation de connexion pour chaque numéro de téléphone avec lequel vous souhaitez utiliser **TextSecure**. Pour ce faire :

Étape 1. Allez dans *Menu*, et **cliquez** sur *secure session* (session sécurisée)



Graphique 8 : Options du menu

Étape 2. Entrez ou sélectionnez le contact souhaité pour **initier l'échange de clés**

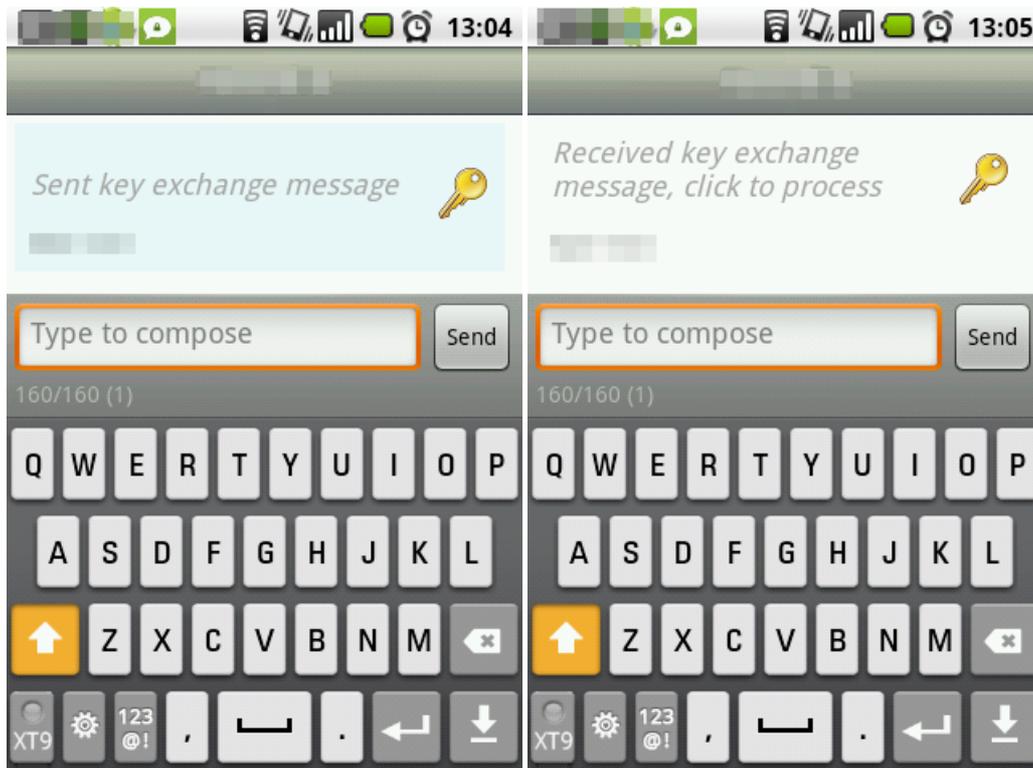


Graphiques 9 et 10 : Lancement de la session sécurisée.

Étape 3. Appuyez sur *send* (envoyer).

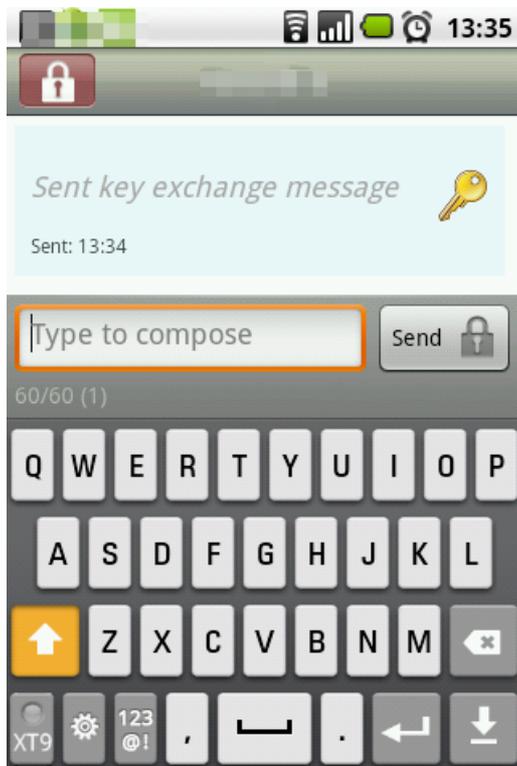
Votre application **TextSecure** va envoyer un message au destinataire dont la propre application **TextSecure** va répondre **AUTOMATIQUEMENT** avec le message d'établir une **connexion sécurisée**. Cette procédure doit être effectuée avec

tous les numéros de téléphone ou contacts.



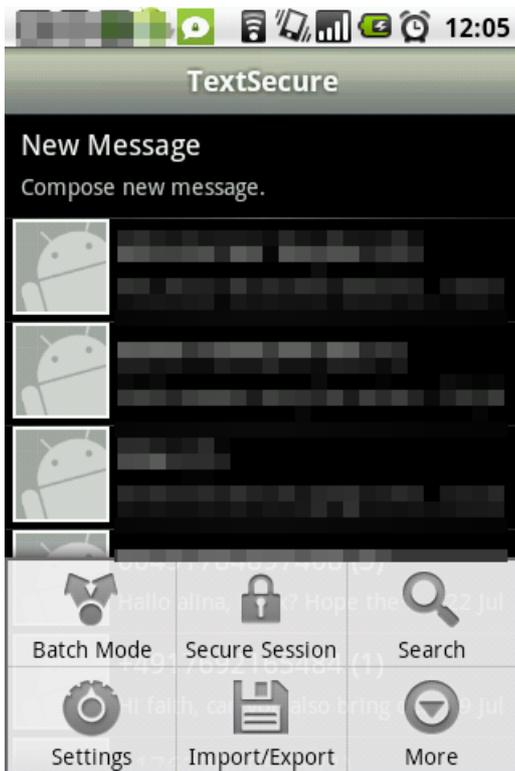
Graphiques 11 et 12 : Messages d'échange de clés.

Étape 4. Lorsque la connexion sécurisée avec ce contact est établie, une icône représentant un cadenas verrouillé va apparaître dans le coin supérieur gauche.



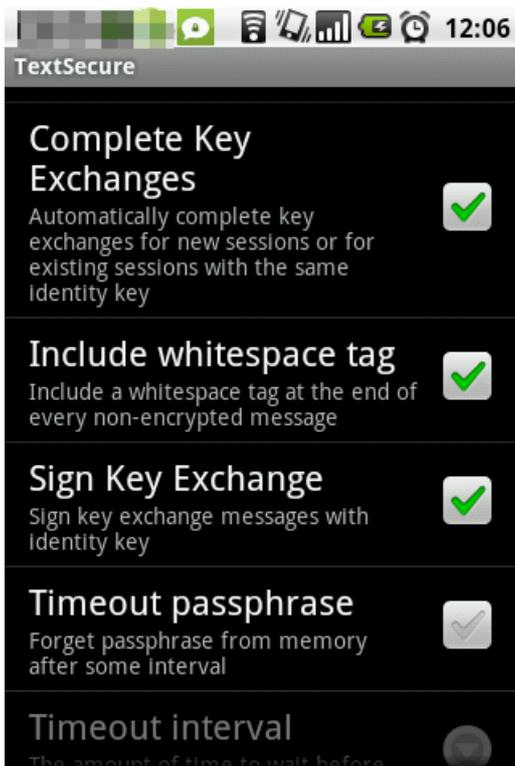
Graphique 12 : Message d'échange de clés envoyé.

Note: Vous pouvez modifier les paramètres pour empêcher **TextSecure** de répondre automatiquement en **sélectionnant** **Menu**, puis **Settings** (paramètres)



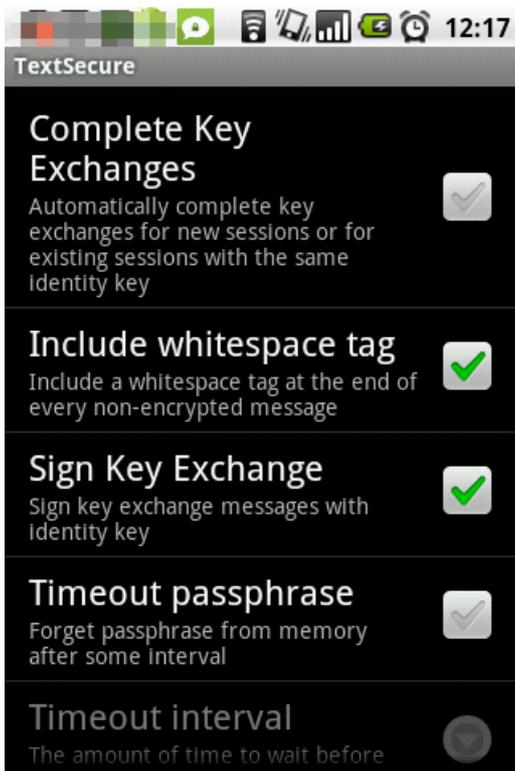
Graphique 13 : Options du menu

Étape 5. Defilez vers le bas jusqu'à *Complete Key Exchanges* (effectuer l'échange de clés). Cette option permet d'effectuer automatiquement les échanges de clés pour les nouvelles sessions sécurisées ou pour des sessions existantes avec la même clé d'identité.



Graphique 14 : Paramètres.

Étape 6. Décochez la case pour désactiver cette option comme ci-dessous.

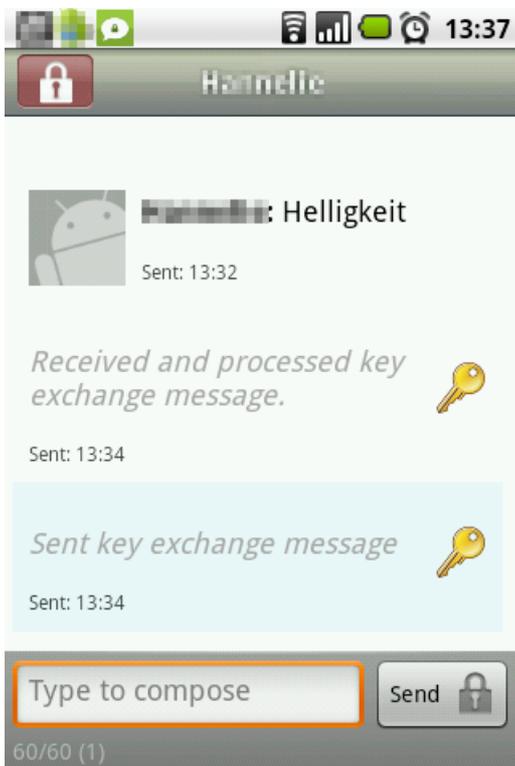


Graphique 15 : Effectuer les échanges de clé désactivé.

2.3 Vérification de l'identité

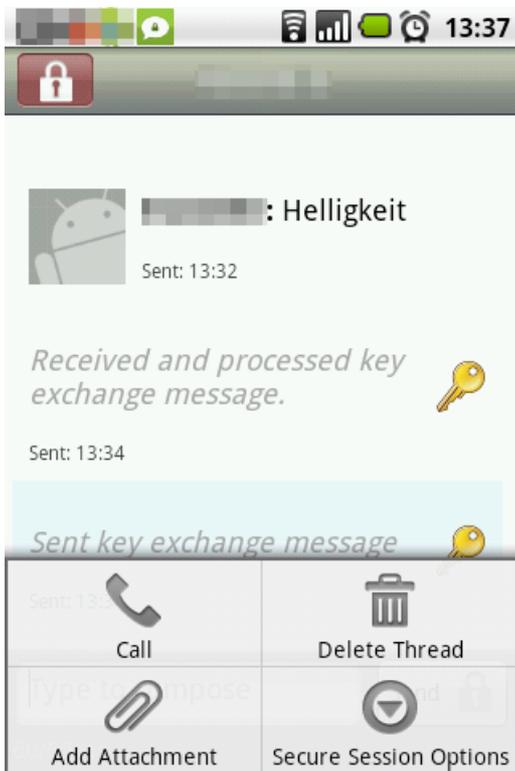
Pour vérifier si vous êtes connecté avec la personne voulue, vous pouvez suivre ces étapes.

Étape 1. Sélectionnez le SMS envoyé automatiquement par **TextSecure** pour établir une connexion sécurisée.



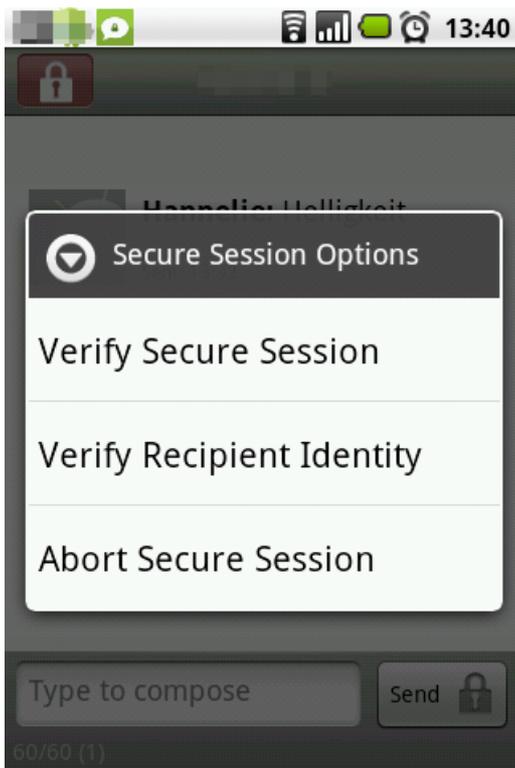
Graphique 16 : Exemple de SMS sélectionné

Étape 2. Sélectionnez Menu puis appuyez sur *Secure Session Options* (options Session sécurisée) pour activer l'écran suivant :



Graphique 17 : Options du menu

Étape 3. Appuyez sur *Verify Recipient Identity* (vérifier l'identité du destinataire). Un ensemble de caractères va s'afficher sur votre téléphone tout comme sur celui de l'autre personne.



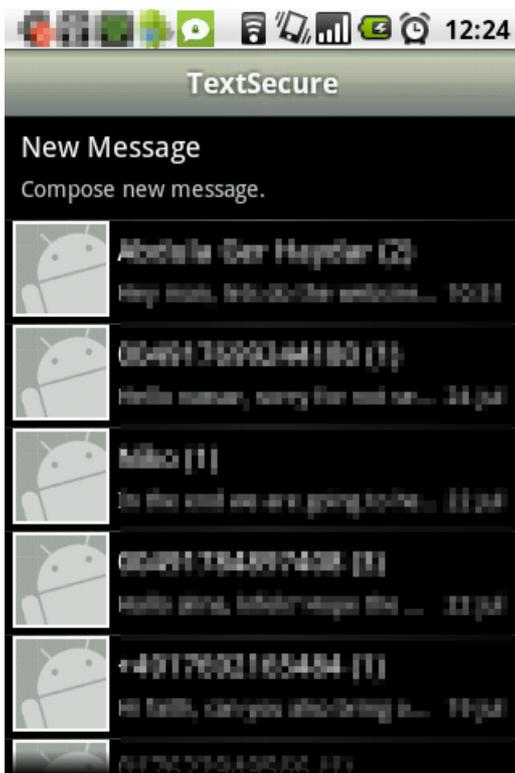
Graphique 18 : Options Session sécurisée.

Étape 4. Contactez l'autre personne (par téléphone ou toute autre voie sécurisée) et confirmez que vous voyez bien le même ensemble de caractères.

2.3 Échanger des messages chiffrés

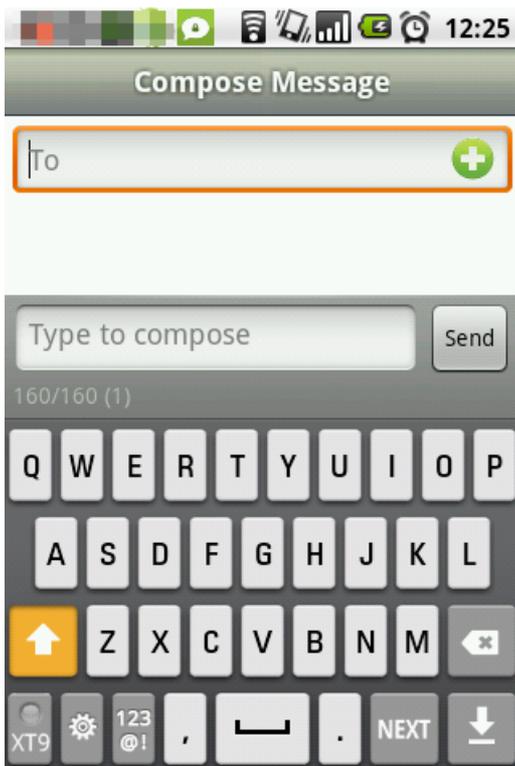
Étape 1. Appuyez sur l'icône **TextSecure**.

Étape 2. Composez un nouveau message.



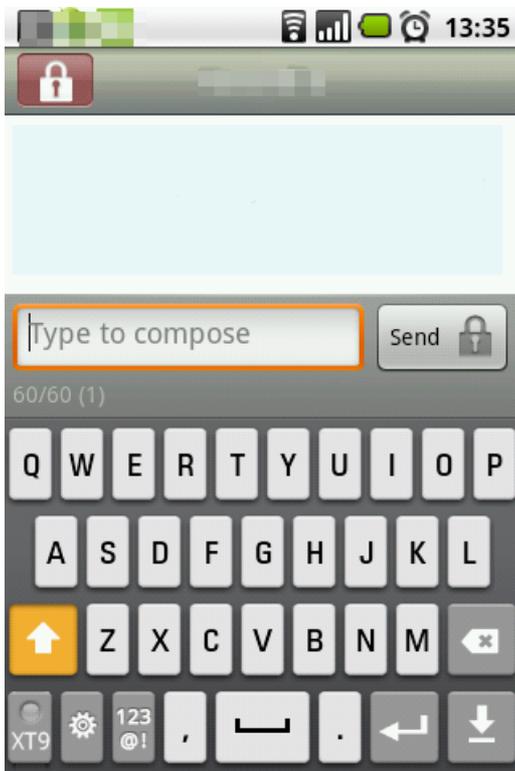
Graphique 19 : Écran d'accueil.

Étape 3. Sélectionnez le contact souhaité.



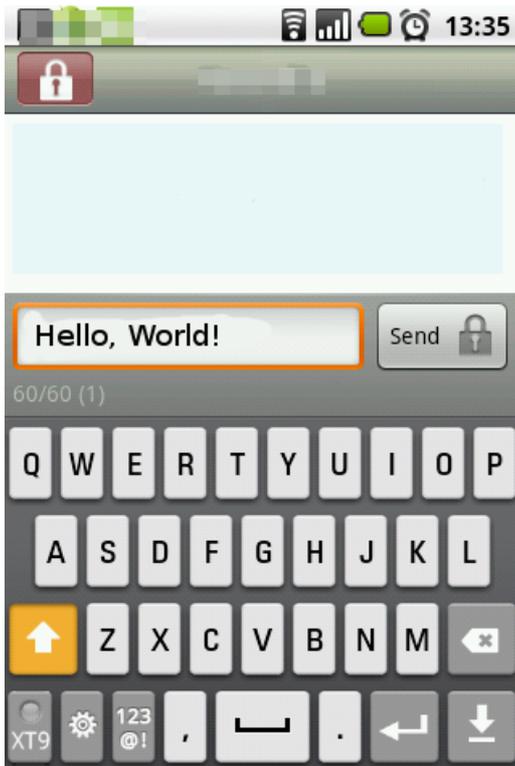
Graphique 20 : Champ de sélection du contact.

Étape 4. Vérifiez que le cadenas apparaît bien dans la touche d'envoi ; ce qui confirme que votre message va être sécurisé.



Graphique 21 : Champ de composition de message

Étape 5. Écrivez le message.



Graphique 22 : Exemple de message.

Étape 6. Cliquez sur *Send* (envoyer).

Important : Si le cadenas n'apparaît pas à côté de la touche d'envoi pendant que vous écrivez votre message, cela signifie que celui-ci va être envoyé en texte brut. Il pourra être intercepté et enregistré en chemin.

URL source (Obtenu le 10/04/2014 - 10:35): <https://securityinabox.org/fr/portablesecurity>

Liens:

[1] <http://www.thialfihar.org/>

[2] <https://securityinabox.org/fr/node/2971>

[3] <https://securityinabox.org/fr/handsonguides>

[4] <http://f-droid.org/>

[5] <http://www.thialfihar.org/projects/apg/>
[6] <https://code.google.com/p/android-privacy-guard/>
[7] <https://securityinabox.org/fr/chapter-3>
[8] <https://securityinabox.org/fr/chapter-7>
[9] <https://securityinabox.org/fr/node/1899>
[10] <https://securityinabox.org/fr/chapter-11>
[11] https://securityinabox.org/fr/chapter_7_4
[12] <https://play.google.com/store/apps/details?id=org.thialfihar.android.apg>
[13] <https://code.google.com/p/cryptonite/>
[14] <https://securityinabox.org/fr/chapter-8>
[15] <https://play.google.com/store/apps/details?id=csh.cryptonite>
[16] <https://guardianproject.info/>
[17] <https://securityinabox.org/fr/glossaire#OTR>
[18] <https://securityinabox.org/fr/glossaire#Pidgin>
[19] <https://securityinabox.org/en/glossary#Orbot>
[20] <https://securityinabox.org/fr/glossaire#Tor>
[21] <https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im>
[22] <https://guardianproject.info/apps/>
[23] <https://guardianproject.info/apps/gibber/>
[24] <https://github.com/guardianproject/gibberbot>
[25] https://securityinabox.org/fr/pidgin_googletalk
[26] <https://securityinabox.org/fr/node/3005>
[27] <https://code.google.com/p/k9mail/>
[28] <https://code.google.com/p/k9mail>
[29] <https://securityinabox.org/fr/node/1945>
[30] <https://play.google.com/store/apps/details?id=com.fsck.k9>
[31] <https://play.google.com/store/apps/details?id=com.android.keepass>
[32] <http://www.keepass.info/download.html>
[33] <http://www.keepassdroid.com>
[34] https://securityinabox.org/fr/keepass_principale
[35] https://securityinabox.org/fr/keepass_motsdepasse
[36] https://security.ngoinabox.org/en/keepass_portable
[37] <https://play.google.com/store/apps/details?id=org.witness.sscphase1>
[38] <https://guardianproject.info/apps/obscuracam/>
[39] <https://github.com/guardianproject/SecureSmartCam>
[40] <https://play.google.com/store/apps/details?id=org.witness.sscphase1&hl=en>
[41] <https://play.google.com/store/apps/details?id=org.torproject.android>
[42] <http://guardianproject.info/apps/orbot/>
[43] <https://securityinabox.org/fr/glossaire>
[44] <https://securityinabox.org/fr/fr/chapter-8>
[45] https://securityinabox.org/fr/fr/chapter_11_7
[46] <https://securityinabox.org/fr/node/2973>
[47] <https://securityinabox.org/fr/node/2970>
[48] https://securityinabox.org/en/Orbot_main
[49] <https://play.google.com/store/apps/details?id=info.guardianproject.browser>
[50] <https://guardianproject.info/apps/orweb/>
[51] <https://market.android.com/details?id=info.guardianproject.browser>
[52] <https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms>
[53] <http://www.whispersys.com>
[54] <http://www.whispersys.com/>
[55] <https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms&hl=en>